Time	TID	Caller	API	Arguments	Status	Return	Repeated
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76bd9000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76bd9000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: C:\WINDOWS\system32\rpcss.dll	failed	DLL_NOT_FOUND	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtQuerySystemInformation**	SystemInformationClass: SystemBasicInformation	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtOpenSection**	DesiredAccess: 0x0000000f ObjectAttributes: kernel.appcore.dll SectionHandle: 0x000001e4	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x73ffc000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x73ff9000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001e4	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x73ff9000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: DDRAW.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D8.DLL	failed	DLL_NOT_FOUND	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D9.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\kernel.appcore.dll DesiredAccess: READ_CONTROL FileHandle: 0x000001e4	success	0x00000000	

2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001e4	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x75013000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x75013000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76cf3000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76cf3000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x75013000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x75013000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**CreateWindowExW**	Style: 0x88000000 Height: 2147483648 ClassName: 49211 Width: 2147483648 WindowName: OleMainThreadWndName y: 2147483648 x: 2147483648	success	0x00000001	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: C:\Windows\System32\uxtheme.dll	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001d4	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtAddAtomEx**	AtomName: OleDropTargetInterface Atom: 0x0000c01e	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtAddAtomEx**	AtomName: OleDropTargetMarshalHwnd Atom: 0x0000c01f	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: OLEAUT32.DLL	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**GetSystemInfo**		success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00006000 NewAccessProtection: PAGE_EXECUTE_READ	success	0x00000000	

				MemoryType: 0x00020000 ProcessHandle: 0xffffffff BaseAddress: 0x00540000			
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtAddAtomEx**	AtomName: VBDisabled Atom: 0x0000c092	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x751b0000 FileName: oleaut32.dll	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x75050000 FileName: ole32.dll	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtQueryValueKey**	FullName: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\SafeProcessSearchMode KeyHandle: 0x000000c8 ValueName: SafeProcessSearchMode	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtQueryAttributesFile**	FileName: C:\Users\Administrator\AppData\Local\Temp\kiato.exe.cfg	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: SXS.DLL	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76c2e000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76c2e000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76c2e000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76c2e000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76c2e000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76c2e000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76c2e000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000	success	0x00000000	

				NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76c2e000			
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76c2e000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76c2e000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x74990000 FileName: USER32	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x00000000 0x00000000	**GetSystemMetrics**	SystemMetricIndex: 0	success	0x00000500	
2019-04-18 21:18:19,550	5280	0x00000000 0x00000000	**GetSystemMetrics**	SystemMetricIndex: 78	success	0x00000500	
2019-04-18 21:18:19,550	5280	0x00000000 0x00000000	**GetSystemMetrics**	SystemMetricIndex: 1	success	0x00000320	
2019-04-18 21:18:19,550	5280	0x00000000 0x00000000	**GetSystemMetrics**	SystemMetricIndex: 79	success	0x00000320	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**CreateWindowExA**	Style: 0x80090000 Height: 0 ClassName: ThunderRT6Main Width: 0 WindowName: y: 2147483648 x: 2147483648	success	0x00000001	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtOpenSection**	DesiredAccess: 0x0000000f ObjectAttributes: MSCTF.dll SectionHandle: 0x000001d0	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74194000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74190000	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001d0	success	0x00000000	
2019-04-18 21:18:19,550	5280	0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no	success	0x00000000	

		0x00000000		OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74190000			
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: DDRAW.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D8.DLL	failed	DLL_NOT_FOUND	
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D9.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:19,550	5280	0x0040122a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\msctf.dll DesiredAccess: READ_CONTROL FileHandle: 0x000001d0	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001d0	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7420e000	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7420e000	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001c8	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7420e000	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7420e000	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76c2e000	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76c2e000	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtOpenKey**	ObjectAttributes: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Codepage DesiredAccess: KEY_READ KeyHandle: 0x000001ec ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \Registry\Machine\System\CurrentControlSet\Control\Nls\Codepage	success	0x00000000	

2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtQueryValueKey**	Information: c_932.nls KeyHandle: 0x000001ec ValueName: 932 Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\932	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtQueryAttributesFile**	FileName: C:\WINDOWS\sysnative\C_932.NLS	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtQueryValueKey**	Information: c_949.nls KeyHandle: 0x000001ec ValueName: 949 Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\949	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtQueryAttributesFile**	FileName: C:\WINDOWS\sysnative\C_949.NLS	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtQueryValueKey**	Information: c_950.nls KeyHandle: 0x000001ec ValueName: 950 Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\950	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtQueryAttributesFile**	FileName: C:\WINDOWS\sysnative\C_950.NLS	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtQueryValueKey**	Information: c_936.nls KeyHandle: 0x000001ec ValueName: 936 Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\936	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtQueryAttributesFile**	FileName: C:\WINDOWS\sysnative\C_936.NLS	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VBA\Monitors DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000000ec ObjectAttributesName: SOFTWARE\Microsoft\VBA\Monitors	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**SetWindowsHookExA**	ProcedureAddress: 0x66061e09 HookIdentifier: WH_MSGFILTER ModuleAddress: 0x00000000 ThreadId: 5280	success	0x0004036b	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**CreateWindowExA**	Style: 0x80000000 Height: 2147483648 ClassName: VBMsoStdCompMgr Width: 2147483648 WindowName: y: 2147483648 x: 2147483648	success	0x00000001	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**CreateWindowExA**	Style: 0x40000000 Height: 0 ClassName: VBFocusRT6 Width: 0 WindowName: y: 0 x: 0	success	0x00000001	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtOpenKey**	ObjectAttributes: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager DesiredAccess: KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS KeyHandle: 0x000001c8 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtQueryValueKey**	FullName: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\ResourcePolicies KeyHandle: 0x000001c8 ValueName: ResourcePolicies	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001c8	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_EXECUTE_READ NumberOfBytesProtected: 0x00006000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x00020000 ProcessHandle: 0xffffffff BaseAddress: 0x00540000	success	0x00000000	
2019-04-18 21:18:19,565	5280	0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no	success	0x00000000	

<table>
<tr><td></td><td></td><td>0x00000000</td><td></td><td>OldAccessProtection: PAGE_READWRITE
NumberOfBytesProtected: 0x0000a000
NewAccessProtection: PAGE_EXECUTE_READ
MemoryType: 0x00020000
ProcessHandle: 0xffffffff
BaseAddress: 0x00540000</td><td></td><td></td><td></td></tr>
<tr><td>2019-04-18 21:18:19,565</td><td>5280</td><td>0x0040122a
0x00000000</td><td>NtOpenKeyEx</td><td>ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VBA\Monitors
DesiredAccess: MAXIMUM_ALLOWED
KeyHandle: 0x00000000
ObjectAttributesHandle: 0x000000ec
ObjectAttributesName: SOFTWARE\Microsoft\VBA\Monitors</td><td>failed</td><td>OBJECT_NAME_NOT
_FOUND</td><td></td></tr>
<tr><td>2019-04-18 21:18:19,565</td><td>5280</td><td>0x00405607
0x0040122a</td><td>LdrLoadDll</td><td>Flags: 0x00000000
BaseAddress: 0x00000000
FileName: user32</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:20,721</td><td>5280</td><td>0x0040122a
0x00000000</td><td>LdrLoadDll</td><td>Flags: 0x00000000
BaseAddress: 0x00000000
FileName: kernel32</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:20,721</td><td>5280</td><td>0x004055b7
0x0040122a</td><td>LdrLoadDll</td><td>Flags: 0x00000000
BaseAddress: 0x00000000
FileName: user32</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:20,721</td><td>5280</td><td>0x0040122a
0x00000000</td><td>NtOpenFile</td><td>ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE
FileName: C:\Users\Administrator\AppData\Local\Temp\
DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE
FileHandle: 0x000001f0</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:20,721</td><td>5280</td><td>0x0040122a
0x00000000</td><td>NtClose</td><td>Handle: 0x000001f0</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:20,721</td><td>5280</td><td>0x0040122a
0x00000000</td><td>LdrLoadDll</td><td>Flags: 0x00000000
BaseAddress: 0x00000000
FileName: kernel32</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:20,721</td><td>5280</td><td>0x00000000
0x00000000</td><td>NtCreateFile</td><td>ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE
FileName: C:\Users\Administrator\AppData\Local\Temp\kiato.exe
DesiredAccess: GENERIC_READ|FILE_READ_ATTRIBUTES|SYNCHRONIZE
ExistedBefore: yes
StackPivoted: no
CreateDisposition: FILE_OPEN_IF
FileHandle: 0x000001c8
FileAttributes: FILE_ATTRIBUTE_NORMAL</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:20,721</td><td>5280</td><td>0x00000000

0x00000000</td><td>NtReadFile</td><td>Buffer:MZ\x90\x00\x03\x00\x00\x00\x04\x00\x00\x00\xff\xff\x00\x00\xb8\x00\x00\x00\x00\x00\x00\x00@\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\xb0\x00\x00\x00\x0e\x1f\xba\x0e\x00\xb4 \xcd!\xb8\x01L\xcd!This program cannot be run in DOS mode.
$\x00\x00\x00\x00\x00\x00\x00\xc9\xe1\x07\xdb\x8d\x80i\x88\x8d\x80i\x88\x8d\x80i\x88\xbb\xa6d\x88\x8c\x80i\x88Ric
h\x8d\x80i\x88\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00PE\x00\x00L\x01\x03\x00\x0f:\xadO\x
00\x00\x00\x00\x00\x00\x00\x00\xe0\x00\x0f\x01\x0b\x01\x06\x00\x00\xb0\x02\x00\x00\xf0\x01\x00\x00\x00\x00\x00
\x12\x00\x00\x00\x10\x00\x00\x00\xc0\x02\x00\x00\x00@\x00\x00\x10\x00\x00\x00\x10\x00\x00\x04\x00\x00\x00\x03\x00
\x08\x00\x04\x00\x00\x00\x00\x00\x00\x00

HandleName: C:\Users\Administrator\AppData\Local\Temp\kiato.exe
Length: 307200
FileHandle: 0x000001c8</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:20,721</td><td>5280</td><td>0x0040122a
0x00000000</td><td>NtClose</td><td>Handle: 0x000001c8</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:20,721</td><td>5280</td><td>0x0040122a
0x00000000</td><td>LdrLoadDll</td><td>Flags: 0x00000000
BaseAddress: 0x00000000
FileName: kernel32</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:20,721</td><td>5280</td><td>0x00000000
0x00000000</td><td>NtCreateFile</td><td>ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE
FileName: C:\Users\Administrator\AppData\Local\Temp\kiato.exe
DesiredAccess: GENERIC_READ|FILE_READ_ATTRIBUTES|SYNCHRONIZE
ExistedBefore: yes
StackPivoted: no
CreateDisposition: FILE_OPEN_IF
FileHandle: 0x000001c8
FileAttributes: FILE_ATTRIBUTE_NORMAL</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:20,721</td><td>5280</td><td>0x0040122a
0x00000000</td><td>NtSetInformationFile</td><td>FileInformationClass: FilePositionInformation
HandleName: C:\Users\Administrator\AppData\Local\Temp\kiato.exe
FileInformation: \xde\x93\x00\x00\x00\x00\x00\x00
FileHandle: 0x000001c8</td><td>success</td><td>0x00000000</td><td></td></tr>
</table>

2019-04-18 21:18:20,721	5280	0x00000000 0x00000000	**NtReadFile**	Buffer: TG{\x9b\x89I:\x90M\x04\x0cx\xb6x\x15\x90\xe5\xf6VW\x95q\xe1>,\xa9\xd0@ \x0b\x13\xc5\xc7\xe3\x1d\x8aM\x0c\x96T3\xb9\x93/(\xe1\x95\xab"s\xe2ajc4\xc7\xf3&\xe5\xd4o.\xcb\xe3j.>\xddk9rg\x851\x9e\x95\xb7 O0\xdeW\xc3ui\x17\xae\xca \xcc\x7f\xb19s\x1a\xe1N[g\x93\x0cz\x00\xd8\x02\xb10\x13E\xfdf\xc9\x8bR\x99q\x86\xe1\xc9\xcf\x8d\x9e\x08/\xed2]\xe1\x96AX\xd12\xdeP\xfd \x0b\xf3(\xa6\xcbn\x0bD\xc1,\xac\xa0\xf3K\xcb3\x83\xfa\xc5"\x85\x17>\x0c\xeb%\xdcB\x08\xfb\x05\xb5\x03\x0b\xe9\x1a\x98z\xdf>p?\xdd\xdd\x8d=tU\xb7)k\x04(\xe8\x9cC\x84O`\xd5Qx\x16\xc7\x08|!m\xeb \xf1\x00\xd9yC_\x99\x01\x8c\xb1\x80\x0f\xc6\xbfC\xf5"\xbb\x89"q\x01\x11\xa5\x0cjl\xf3\xfd\xbe\xa194\x97\xa8#yAn\x9b\x9b\x1b\xc8B\x8fR \xff\x91 HandleName: C:\Users\Administrator\AppData\Local\Temp\kiato.exe Length: 1672 FileHandle: 0x000001c8	success	0x00000000	
2019-04-18 21:18:20,721	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001c8	success	0x00000000	
2019-04-18 21:18:20,987	5280	0x0040122a 0x00000000	**GetLocalTime**		success	0x00000000	
2019-04-18 21:18:21,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:21,003	5280	0x0061e430 0x0040122a	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:21,003	5280	0x0061e430 0x0040122a	**NtDelayExecution**	Milliseconds: 1000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: shell32	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenSection**	DesiredAccess: 0x0000000f ObjectAttributes: shell32.DLL SectionHandle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00002000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x757ba000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00002000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x757b0000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenSection**	DesiredAccess: 0x0000000f ObjectAttributes: cfgmgr32.dll SectionHandle: 0x000001c8	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74c15000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY	success	0x00000000	

				NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000			
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74c13000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001c8	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenSection**	DesiredAccess: 0x0000000f ObjectAttributes: shcore.dll SectionHandle: 0x000001c8	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7667d000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7667a000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001c8	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenSection**	DesiredAccess: 0x0000000f ObjectAttributes: windows.storage.dll SectionHandle: 0x000001c8	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000	success	0x00000000	

				ProcessHandle: 0xffffffff BaseAddress: 0x7782b000			
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7476f000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenSection**	DesiredAccess: 0x0000000f ObjectAttributes: shlwapi.dll SectionHandle: 0x000001f0	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x752a0000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7529c000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001f0	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenSection**	DesiredAccess: 0x0000000f ObjectAttributes: profapi.dll SectionHandle: 0x000001f0	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76ea5000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00003000	success	0x00000000	

				NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000			
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76ea3000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001f0	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenSection**	DesiredAccess: 0x0000000f ObjectAttributes: powrprof.dll SectionHandle: 0x000001f0	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76709000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76707000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001f0	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenSection**	DesiredAccess: 0x0000000f ObjectAttributes: FLTLIB.DLL SectionHandle: 0x000001f0	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff	success	0x00000000	

				BaseAddress: 0x74985000			
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001f0	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001c8	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00002000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x757b0000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74c13000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7667a000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7529c000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76ea3000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x76707000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74985000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7476f000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: DDRAW.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D8.DLL	failed	DLL_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D9.DLL	failed	DLL_NOT_FOUND	1 time

2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\cfgmgr32.dll DesiredAccess: READ_CONTROL FileHandle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: DDRAW.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D8.DLL	failed	DLL_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D9.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\SHCore.dll DesiredAccess: READ_CONTROL FileHandle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: DDRAW.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D8.DLL	failed	DLL_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D9.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\shlwapi.dll DesiredAccess: READ_CONTROL FileHandle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: DDRAW.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D8.DLL	failed	DLL_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D9.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\profapi.dll DesiredAccess: READ_CONTROL FileHandle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: DDRAW.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D8.DLL	failed	DLL_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D9.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\powrprof.dll DesiredAccess: READ_CONTROL FileHandle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: DDRAW.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D8.DLL	failed	DLL_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D9.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\fltLib.dll DesiredAccess: READ_CONTROL FileHandle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: DDRAW.DLL	failed	DLL_NOT_FOUND	1 time

2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D8.DLL	failed	DLL_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D9.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\windows.storage.dll DesiredAccess: READ_CONTROL FileHandle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: DDRAW.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D8.DLL	failed	DLL_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D9.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\shell32.dll DesiredAccess: READ_CONTROL FileHandle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001cc	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtCreateFile**	ShareAccess: 0 FileName: \Device\DeviceApi\CMApi DesiredAccess: GENERIC_READ ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x000001cc FileAttributes: 0x00000000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x76d00000 FileName: advapi32.dll	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x77710000 FileName: ntdll.dll	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtOpenSection**	DesiredAccess: 0x00000006 ObjectAttributes: windows_shell_global_counters SectionHandle: 0x00000278	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE	success	0x00000000	

				MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000			
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtOpenKeyEx**	ObjectAttributes:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions DesiredAccess: KEY_READ KeyHandle: 0x00000280 ObjectAttributesHandle: 0x000000ec ObjectAttributesName: Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtOpenKeyEx**	ObjectAttributes:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173} DesiredAccess: KEY_READ KeyHandle: 0x00000284 ObjectAttributesHandle: 0x00000280 ObjectAttributesName: {5E6C858F-0E22-4760-9AFE-EA3317B67173}	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtClose**	Handle: 0x00000280	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	Information: 2 KeyHandle: 0x00000284 ValueName: Category Type: REG_DWORD FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Category	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	Information: Profile KeyHandle: 0x00000284 ValueName: Name Type: REG_SZ FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Name	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\ParentFolder KeyHandle: 0x00000284 ValueName: ParentFolder	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Description KeyHandle: 0x00000284 ValueName: Description	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\RelativePath KeyHandle: 0x00000284 ValueName: RelativePath	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\ParsingName KeyHandle: 0x00000284 ValueName: ParsingName	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\InfoTip KeyHandle: 0x00000284 ValueName: InfoTip	failed	OBJECT_NAME_NOT_FOUND	

2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\LocalizedName KeyHandle: 0x00000284 ValueName: LocalizedName	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Icon KeyHandle: 0x00000284 ValueName: Icon	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Security KeyHandle: 0x00000284 ValueName: Security	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\StreamResource KeyHandle: 0x00000284 ValueName: StreamResource	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\StreamResourceType KeyHandle: 0x00000284 ValueName: StreamResourceType	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\LocalRedirectOnly KeyHandle: 0x00000284 ValueName: LocalRedirectOnly	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Roamable KeyHandle: 0x00000284 ValueName: Roamable	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PreCreate KeyHandle: 0x00000284 ValueName: PreCreate	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Stream KeyHandle: 0x00000284 ValueName: Stream	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PublishExpandedPath KeyHandle: 0x00000284 ValueName: PublishExpandedPath	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\DefinitionFlags KeyHandle: 0x00000284 ValueName: DefinitionFlags	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Attributes KeyHandle: 0x00000284 ValueName: Attributes	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\FolderTypeID KeyHandle: 0x00000284 ValueName: FolderTypeID	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\InitFolderHandler KeyHandle: 0x00000284 ValueName: InitFolderHandler	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtOpenKeyEx**	ObjectAttributes:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PropertyBag DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000284 ObjectAttributesName: PropertyBag	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtClose**	Handle: 0x00000284	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000	success	0x00000000	

				ProcessHandle: 0xffffffff BaseAddress: 0x74775000			
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2035269069-1835038330-1888751347-500 DesiredAccess: KEY_READ KeyHandle: 0x00000280 ObjectAttributesHandle: 0x000000ec ObjectAttributesName: Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2035269069-1835038330-1888751347-500	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2035269069-1835038330-1888751347-500\ProfileImagePath KeyHandle: 0x00000280 ValueName: ProfileImagePath	failed	BUFFER_OVERFLOW	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryValueKey**	Information: C:\Users\Administrator KeyHandle: 0x00000280 ValueName: ProfileImagePath Type: REG_EXPAND_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2035269069-1835038330-1888751347-500\ProfileImagePath	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtClose**	Handle: 0x00000280	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtClose**	Handle: 0x00000284	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtClose**	Handle: 0x0000027c	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**LdrGetDllHandle**	ModuleHandle: 0x77710000 FileName: ntdll.dll	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: C:\Users\Administrator DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_CREATE FileHandle: 0x00000000 FileAttributes: FILE_ATTRIBUTE_NORMAL	failed	OBJECT_NAME_COLLISION	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtQueryAttributesFile**	FileName: C:\Users\Administrator	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e64f 0x0040122a	**NtOpenKeyEx**	ObjectAttributes:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\KnownFolderSettings DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000000ec ObjectAttributesName: Software\Microsoft\Windows\CurrentVersion\Explorer\KnownFolderSettings	failed	OBJECT_NAME_NOT_FOUND	1 time
2019-04-18 21:18:22,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: shell32	success	0x00000000	
2019-04-18 21:18:22,018	5280	0x0061e43f 0x0040122a	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: C:\Users\Administrator DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE	failed	OBJECT_NAME_COLLISION	

<table>
<tr><td></td><td></td><td></td><td></td><td>ExistedBefore: yes
StackPivoted: no
CreateDisposition: FILE_CREATE
FileHandle: 0x00000000
FileAttributes: FILE_ATTRIBUTE_NORMAL</td><td></td><td></td><td></td></tr>
<tr><td>2019-04-18 21:18:22,018</td><td>5280</td><td>0x0061e43f
0x0040122a</td><td>NtQueryAttributesFile</td><td>FileName: C:\Users\Administrator</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:22,018</td><td>5280</td><td>0x0040122a
0x00000000</td><td>LdrLoadDll</td><td>Flags: 0x00000000
BaseAddress: 0x00000000
FileName: advapi32</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:22,018</td><td>5280</td><td>0x0061e435
0x0040122a</td><td>GetUserNameW</td><td>Name: Administrator</td><td>success</td><td>0x00000001</td><td></td></tr>
<tr><td>2019-04-18 21:18:22,018</td><td>5280</td><td>0x0040122a
0x00000000</td><td>LdrLoadDll</td><td>Flags: 0x00000000
BaseAddress: 0x00000000
FileName: kernel32</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:22,034</td><td>5280</td><td>0x0061e43a
0x0040122a</td><td>NtOpenMutant</td><td>Handle: 0x00000000
MutexName: A</td><td>failed</td><td>OBJECT_NAME_NOT_FOUND</td><td></td></tr>
<tr><td>2019-04-18 21:18:22,034</td><td>5280</td><td>0x0040122a
0x00000000</td><td>LdrLoadDll</td><td>Flags: 0x00000000
BaseAddress: 0x00000000
FileName: kernel32</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:22,034</td><td>5280</td><td>0x0061e43a
0x0040122a</td><td>NtCreateMutant</td><td>Handle: 0x0000027c
InitialOwner: 1
MutexName: A</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:22,034</td><td>5280</td><td>0x0040122a
0x00000000</td><td>LdrLoadDll</td><td>Flags: 0x00000000
BaseAddress: 0x00000000
FileName: kernel32</td><td>success</td><td>0x00000000</td><td>1 time</td></tr>
<tr><td>2019-04-18 21:18:22,034</td><td>5280</td><td>0x0061e430
0x0040122a</td><td>NtClose</td><td>Handle: 0x0000027c</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:22,034</td><td>5280</td><td>0x0040122a
0x00000000</td><td>LdrLoadDll</td><td>Flags: 0x00000000
BaseAddress: 0x00000000
FileName: kernel32</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:22,034</td><td>5280</td><td>0x0040122a
0x00000000</td><td>NtOpenFile</td><td>ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE
FileName: C:\Users\Administrator\AppData\Local\Temp\
DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE
FileHandle: 0x0000027c</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:22,034</td><td>5280</td><td>0x0040122a
0x00000000</td><td>NtClose</td><td>Handle: 0x0000027c</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:22,034</td><td>5280</td><td>0x00000000
0x00000000</td><td>NtCreateFile</td><td>ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE
FileName: C:\Users\Administrator\AppData\Local\Temp\kiato.exe
DesiredAccess: GENERIC_READ|FILE_READ_ATTRIBUTES|SYNCHRONIZE
ExistedBefore: yes
StackPivoted: no
CreateDisposition: FILE_OPEN_IF
FileHandle: 0x0000027c
FileAttributes: FILE_ATTRIBUTE_NORMAL</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:22,034</td><td>5280</td><td>0x00000000
0x00000000</td><td>NtReadFile</td><td>Buffer:MZ\x90\x00\x03\x00\x00\x00\x04\x00\x00\x00\xff\xff\x00\x00\xb8\x00\x00\x00\x00\x00\x00\x00@\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xb0\x00\x00\x00\x0e\x1f\xba\x0e\x00\xb4 \xcd!\xb8\x01L\xcd!This program cannot be run in DOS mode.
$\x00\x00\x00\x00\x00\x00\x00\xc9\xe1\x07\xdb\x8d\x80i\x88\x8d\x80i\x88\x8d\x80i\x88\xbb\xa6d\x88\x8c\x80i\x88Rich\x8d\x80i\x88\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00PE\x00\x00L\x01\x03\x00\x0f:\xadO\x00\x00\x00\x00\x00\x00\x00\x00\xe0\x00\x0f\x01\x0b\x01\x06\x00\x00\xb0\x02\x00\x00\xf0\x01\x00\x00\x00\x00\x00\x12\x00\x00\x00\x10\x00\x00\x00\xc0\x02\x00\x00\x00@\x00\x00\x10\x00\x00\x00\x10\x00\x00\x04\x00\x00\x00\x03\x00\x08\x00\x04\x00\x00\x00\x00\x00\x00\x00
HandleName: C:\Users\Administrator\AppData\Local\Temp\kiato.exe
Length: 307200
FileHandle: 0x0000027c</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:22,034</td><td>5280</td><td>0x0040122a
0x00000000</td><td>NtClose</td><td>Handle: 0x0000027c</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:22,300</td><td>5280</td><td>0x00000000
0x00000000</td><td>NtCreateFile</td><td>ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE
FileName: C:\Users\Administrator\suoes.exe
DesiredAccess: GENERIC_WRITE|FILE_READ_ATTRIBUTES|SYNCHRONIZE
ExistedBefore: no
StackPivoted: no
CreateDisposition: FILE_OPEN_IF
FileHandle: 0x000001c4
FileAttributes: FILE_ATTRIBUTE_NORMAL</td><td>success</td><td>0x00000000</td><td></td></tr>
</table>

2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer:MZ\x90\x00\x03\x00\x00\x00\x04\x00\x00\x00\xff\xff\x00\x00\xb8\x00\x00\x00\x00\x00\x00\x00@\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xb0\x00\x00\x00\x0e\x1f\xba\x0e\x00\xb4 \xcd!\xb8\x01L\xcd!This program cannot be run in DOS mode. $\x00\x00\x00\x00\x00\x00\x00\xc9\xe1\x07\xdb\x8d\x80i\x88\x8d\x80i\x88\x8d\x80i\x88\xbb\xa6d\x88\x8c\x80i\x88Rich\x8d\x80i\x88\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00PE\x00\x00L\x01\x03\x00\x0f:\xadO\x00\x00\x00\x00\x00\x00\x00\x00\xe0\x00\x0f\x01\x0b\x01\x06\x00\x00\xb0\x02\x00\x00\xf0\x01\x00\x00\x00\x00\x00 \x12\x00\x00\x00\x10\x00\x00\x00\xc0\x02\x00\x00\x00@\x00\x00\x10\x00\x00\x00\x10\x00\x00\x04\x00\x00\x00\x03\x00 \x08\x00\x04\x00\x00\x00\x00\x00\x00\x00 HandleName: C:\Users\Administrator\suoes.exe Length: 307200 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: C:\Users\Administrator\suoes.exe DesiredAccess: GENERIC_WRITE|FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_OPEN_IF FileHandle: 0x000001c4 FileAttributes: FILE_ATTRIBUTE_NORMAL	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xde\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: p HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdf\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xcc HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe0\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xef HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe1\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xb7 HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe2\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: * HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe3\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xad HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				Length: 1 FileHandle: 0x000001c4			
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe4\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xac HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe5\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: C HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe6\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \x99 HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe7\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \x9d HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe8\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xd0 HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe9\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \x87 HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xea\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer:) HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xeb\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xec\x93\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xd3 HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xed\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: >\ HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xee\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: _ HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xef\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: n HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf0\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: u HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf1\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,300	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xeb HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf2\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: % HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf3\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: 4 HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf4\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: - HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf5\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: % HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf6\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \x7f HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf7\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xcf HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf8\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xb5 HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf9\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: Y HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfa\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: ; HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfb\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xa1 HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfc\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xcc HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfd\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000	**NtWriteFile**	Buffer: \x0f	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4			
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfe\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: U HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xff\x93\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \x83 HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x00\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: L HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x01\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xe2 HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x02\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xfd HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x03\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: T HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x04\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: L HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x05\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xdb HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: \x06\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: k HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x07\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xae HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x08\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xef HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xe0 HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xdb HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x0b\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \xfb HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x0c\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \x87 HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \x8c HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x0e\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,315	5280	0x00000000 0x00000000	**NtWriteFile**	Buffer: \x18 HandleName: C:\Users\Administrator\suoes.exe Length: 1	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,315	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x0f\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x00000000 0x00000000	**NtWriteFile**	Status: Maximum logged writes reached for this file Buffer: Z HandleName: C:\Users\Administrator\suoes.exe Length: 1 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x10\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x11\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x12\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x13\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x14\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x15\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x16\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x17\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x18\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x19\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1a\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1b\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1c\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1d\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1e\x94\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1f\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: !\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: "\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: #\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: $\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: %\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: &\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: '\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: (\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation:)\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: *\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: +\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ,\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: -\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: .\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: /\x94\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 0\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 1\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 2\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 3\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 4\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 5\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 6\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 7\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 8\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 9\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: :\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ;\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: <\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: =\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: >\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ?\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: @\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,331	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: A\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,331	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: B\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: C\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: D\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: E\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: F\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: G\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: H\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: I\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: J\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: K\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: L\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: M\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: N\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: O\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: P\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Q\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: R\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: S\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: T\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: U\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: V\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: W\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: X\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Y\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Z\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: [\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation:]\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ^\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: _\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: `\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: a\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: b\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: c\x94\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: d\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: e\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: f\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: g\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: h\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: i\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: j\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: k\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: l\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: m\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: n\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: o\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: p\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: q\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: r\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: s\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: t\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: u\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: v\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,346	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: w\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: x\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: y\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: z\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: {\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: |\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: }\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ~\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x7f\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x80\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x81\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x82\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x83\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x84\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x85\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x86\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x87\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x88\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x89\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8a\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8b\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8c\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8d\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8e\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8f\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x90\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x91\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x92\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x93\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x94\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x95\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x96\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: \x97\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x98\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x99\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9a\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9b\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9c\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9d\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9e\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9f\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa0\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa1\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa2\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa3\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa4\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa5\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa6\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa7\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa8\x94\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa9\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,362	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xaa\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xab\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xac\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xad\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xae\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xaf\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb0\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb1\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb2\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb3\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb4\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb5\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb6\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb7\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb8\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb9\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xba\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbb\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbc\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbd\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbe\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbf\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc0\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc1\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc2\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc3\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc4\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc5\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc6\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc7\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc8\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc9\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xca\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcb\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcc\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcd\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xce\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcf\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd0\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd1\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd2\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd3\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd4\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd5\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd6\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd7\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd8\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd9\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,378	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xda\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdb\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: \xdc\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdd\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xde\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdf\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe0\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe1\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe2\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe3\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe4\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe5\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe6\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe7\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe8\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe9\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xea\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xeb\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xec\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xed\x94\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xee\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xef\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf0\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf1\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf2\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf3\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf4\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf5\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf6\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf7\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf8\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf9\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfa\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfb\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfc\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfd\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfe\x94\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\xff\x94\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x00\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x01\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x02\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x03\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x04\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x05\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x06\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x07\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x08\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x0b\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x0c\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x0e\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x0f\x95\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation`	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x10\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x11\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x12\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,393	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x13\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x14\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x15\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x16\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x17\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x18\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x19\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1a\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1b\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1c\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1d\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1e\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1f\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: !\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: "\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: #\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: $\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: %\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: &\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: '\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: (\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation:)\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: *\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: +\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ,\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: -\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: .\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: /\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 0\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 1\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 2\x95\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 3\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 4\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 5\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 6\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 7\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 8\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 9\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: :\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ;\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: <\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: =\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: >\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ?\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: @\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: A\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: B\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: C\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: D\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: E\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: F\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: G\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: H\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: I\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: J\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: K\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: L\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: M\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: N\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,409	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: O\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: P\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Q\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: R\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: S\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: T\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: U\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: V\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: W\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: X\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Y\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Z\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: [\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation:]\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ^\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: _\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: `\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: a\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: b\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: c\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: d\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: e\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: f\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: g\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: h\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: i\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: j\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: k\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: l\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: m\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: n\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: o\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: p\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: q\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: r\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: s\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: t\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: u\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: v\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: w\x95\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: x\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: y\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: z\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: {\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: |\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: }\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ~\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x7f\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x80\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x81\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x82\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x83\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x84\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x85\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x86\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x87\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x88\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,425	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x89\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8a\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8b\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8c\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8d\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8e\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8f\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x90\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x91\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x92\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x93\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x94\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x95\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x96\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x97\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x98\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x99\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9a\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9b\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9c\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9d\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9e\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9f\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa0\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa1\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa2\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa3\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa4\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa5\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa6\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa7\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa8\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa9\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xaa\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: \xab\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xac\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xad\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xae\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xaf\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb0\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb1\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb2\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb3\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb4\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb5\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb6\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb7\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb8\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb9\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xba\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbb\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbc\x95\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbd\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbe\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbf\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc0\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc1\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,440	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc2\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc3\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc4\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc5\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc6\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc7\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc8\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc9\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xca\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcb\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcc\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcd\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xce\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcf\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd0\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd1\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd2\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd3\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd4\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd5\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd6\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd7\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd8\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd9\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xda\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdb\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdc\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdd\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xde\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdf\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe0\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe1\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe2\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe3\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe4\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe5\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe6\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe7\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe8\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe9\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xea\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xeb\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xec\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xed\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xee\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xef\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: \xf0\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf1\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf2\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf3\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,456	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf4\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf5\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf6\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf7\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf8\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf9\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfa\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfb\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfc\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfd\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfe\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xff\x95\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x00\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x01\x96\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: `0x000001c4`			
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x02\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x03\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x04\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x05\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x06\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x07\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x08\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x0b\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x0c\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x0e\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x0f\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x10\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x11\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x12\x96\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	

2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x13\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x14\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x15\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x16\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x17\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x18\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x19\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1a\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1b\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1c\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1d\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1e\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1f\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: !\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: "\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,471	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: #\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: $\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: %\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: &\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: '\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: (\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation:)\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: *\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: +\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ,\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: -\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: .\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: /\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 0\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 1\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 2\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 3\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 4\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: 5\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 6\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 7\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 8\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 9\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: :\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ;\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: <\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: =\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: >\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ?\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: @\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: A\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: B\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: C\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: D\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: E\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: F\x96\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: G\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: H\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: I\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: J\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: K\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: L\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: M\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: N\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: O\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: P\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Q\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: R\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: S\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,487	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: T\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: U\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: V\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: W\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: X\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Y\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Z\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: [\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation:]\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ^\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: _\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: `\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: a\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: b\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: c\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: d\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: e\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: f\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: g\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: h\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: i\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: j\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: k\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: l\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: m\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: n\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: o\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: p\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: q\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: r\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: s\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: t\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: u\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: v\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: w\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: x\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: y\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: z\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: {\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: |\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: }\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ~\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x7f\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x80\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x81\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x82\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x83\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x84\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x85\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,503	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x86\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x87\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x88\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x89\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8a\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8b\x96\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8c\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8d\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8e\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8f\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x90\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x91\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x92\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x93\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x94\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x95\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x96\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x97\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x98\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x99\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9a\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9b\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9c\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9d\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9e\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9f\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa0\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa1\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa2\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa3\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa4\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa5\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa6\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa7\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa8\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa9\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xaa\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xab\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xac\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xad\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xae\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xaf\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb0\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb1\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb2\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb3\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb4\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb5\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb6\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb7\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb8\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb9\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,518	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xba\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbb\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbc\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbd\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbe\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: \xbf\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc0\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc1\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc2\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc3\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc4\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc5\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc6\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc7\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc8\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc9\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xca\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcb\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcc\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcd\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xce\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcf\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd0\x96\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd1\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd2\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd3\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd4\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd5\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd6\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd7\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd8\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd9\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xda\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdb\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdc\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdd\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xde\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdf\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe0\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe1\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe2\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe3\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe4\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe5\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe6\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe7\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe8\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe9\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xea\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xeb\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xec\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xed\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xee\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xef\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf0\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf1\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf2\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf3\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf4\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf5\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf6\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf7\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,534	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf8\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf9\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfa\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfb\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfc\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfd\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfe\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xff\x96\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x00\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x01\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x02\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x03\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: \x04\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x05\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x06\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x07\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x08\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x0b\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x0c\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x0e\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x0f\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x10\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x11\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x12\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x13\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x14\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x15\x97\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x16\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x17\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x18\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x19\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1a\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1b\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1c\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1d\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1e\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1f\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: !\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: "\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: #\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: $\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: %\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: &\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: '\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: (\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation:)\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: *\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: +\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ,\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: -\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: .\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: /\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 0\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,550	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 1\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 2\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 3\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 4\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 5\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 6\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 7\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: 8\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 9\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: :\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ;\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: <\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: =\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: >\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ?\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: @\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: A\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: B\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: C\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: D\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: E\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: F\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: G\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: H\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: I\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: J\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: K\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: L\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: M\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: N\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: O\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: P\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Q\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: R\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: S\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: T\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: U\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: V\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: W\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: X\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Y\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Z\x97\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: [\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation:]\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ^\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: _\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: `\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: a\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: b\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: c\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: d\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: e\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: f\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: g\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: h\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: i\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,565	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: j\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: k\x97\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: l\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: m\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: n\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: o\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: p\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: q\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: r\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: s\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: t\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: u\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: v\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: w\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: x\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: y\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: z\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: {\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: |\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: }\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ~\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x7f\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x80\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x81\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x82\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x83\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x84\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x85\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x86\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x87\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x88\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x89\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8a\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8b\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8c\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8d\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: \x8e\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8f\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x90\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x91\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x92\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x93\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x94\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x95\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x96\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x97\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x98\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x99\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9a\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9b\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9c\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9d\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9e\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9f\x97\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa0\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,581	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa1\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa2\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa3\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa4\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa5\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa6\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa7\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa8\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa9\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xaa\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xab\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xac\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xad\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xae\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xaf\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb0\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb1\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb2\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb3\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb4\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb5\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb6\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb7\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb8\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb9\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xba\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbb\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbc\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbd\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbe\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbf\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc0\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc1\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc2\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc3\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc4\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc5\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc6\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc7\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc8\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc9\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xca\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcb\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcc\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcd\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xce\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcf\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd0\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd1\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd2\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: \xd3\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd4\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd5\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd6\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd7\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd8\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd9\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xda\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdb\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdc\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdd\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xde\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdf\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe0\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe1\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe2\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe3\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe4\x97\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe5\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe6\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe7\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,596	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe8\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe9\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xea\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xeb\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xec\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xed\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xee\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xef\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf0\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf1\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf2\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf3\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf4\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf5\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf6\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf7\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf8\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf9\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfa\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfb\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfc\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfd\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfe\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xff\x97\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x00\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x01\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x02\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x03\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x04\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x05\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x06\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x07\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`			
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x08\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x0b\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x0c\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x0e\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x0f\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x10\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x11\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x12\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x13\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x14\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x15\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x16\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x17\x98\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe`	success	`0x00000000`	

				FileInformation: \x18\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x19\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1a\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1b\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1c\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1d\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1e\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1f\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: !\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: "\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: #\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: $\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: %\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: &\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: '\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: (\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation:)\x98\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: *\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: +\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ,\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: -\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: .\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,612	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: /\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 0\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 1\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 2\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 3\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 4\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 5\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 6\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 7\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 8\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 9\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: :\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ;\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: <\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: =\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: >\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ?\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: @\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: A\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: B\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: C\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: D\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: E\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: F\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: G\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: H\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: I\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: J\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: K\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: L\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: M\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: N\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: O\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: P\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Q\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: R\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: S\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: T\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: U\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: V\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: W\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: X\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Y\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Z\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: [\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation:]\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ^\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: _\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: `\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: a\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: b\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: c\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: d\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: e\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: f\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: g\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: h\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: i\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: j\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: k\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: l\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: m\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: n\x98\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: o\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: p\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: q\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: r\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: s\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: t\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: u\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: v\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: w\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: x\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: y\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,628	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: z\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: {\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: |\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: }\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ~\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x7f\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x80\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x81\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x82\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x83\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x84\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x85\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x86\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x87\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x88\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x89\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8a\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8b\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8c\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8d\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8e\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8f\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x90\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x91\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x92\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x93\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x94\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x95\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x96\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x97\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x98\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x99\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9a\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9b\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9c\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9d\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9e\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9f\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa0\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa1\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: \xa2\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa3\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa4\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa5\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa6\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa7\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa8\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa9\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xaa\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xab\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xac\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xad\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xae\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xaf\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb0\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb1\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb2\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb3\x98\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb4\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb5\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb6\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb7\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb8\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb9\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xba\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbb\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbc\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbd\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbe\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbf\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc0\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc1\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc2\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc3\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc4\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc5\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,643	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc6\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc7\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc8\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc9\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xca\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcb\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcc\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcd\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xce\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcf\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd0\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd1\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd2\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd3\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd4\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd5\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd6\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd7\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd8\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd9\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xda\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdb\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdc\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdd\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xde\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdf\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe0\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe1\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe2\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe3\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe4\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe5\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe6\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: \xe7\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe8\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe9\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xea\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xeb\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xec\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xed\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xee\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xef\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf0\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf1\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf2\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf3\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf4\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf5\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf6\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf7\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf8\x98\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf9\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfa\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfb\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfc\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfd\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfe\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xff\x98\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x00\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x01\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x02\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x03\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x04\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x05\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x06\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x07\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x08\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x0b\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x0c\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x0e\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x0f\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x10\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x11\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x12\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x13\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x14\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x15\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x16\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x17\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x18\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x19\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1a\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,659	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1b\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1c\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1d\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1e\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1f\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: !\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: "\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: #\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: $\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: %\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: &\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: '\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: (\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation:)\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: *\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: +\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: ,\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: -\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: .\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: /\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 0\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 1\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 2\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 3\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 4\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 5\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 6\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 7\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 8\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 9\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: :\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ;\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: <\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: =\x99\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: >\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ?\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: @\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: A\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: B\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: C\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: D\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: E\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: F\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: G\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: H\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: I\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: J\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: K\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: L\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: M\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: N\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: O\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: P\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Q\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: R\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: S\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: T\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: U\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: V\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: W\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: X\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Y\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Z\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: [\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation:]\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ^\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: _\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: `\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: a\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: b\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: c\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: d\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: e\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: f\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: g\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: h\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: i\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: j\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,675	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: k\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: l\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: m\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: n\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: o\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: p\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: q\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: r\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: s\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: t\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: u\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: v\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: w\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: x\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: y\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: z\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: {\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: |\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: }\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ~\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x7f\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x80\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x81\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x82\x99\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x83\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x84\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x85\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x86\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x87\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x88\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x89\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8a\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8b\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8c\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8d\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8e\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x8f\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x90\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x91\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x92\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x93\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x94\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x95\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x96\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x97\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x98\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x99\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9a\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9b\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9c\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9d\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9e\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9f\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa0\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa1\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa2\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa3\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa4\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa5\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa6\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa7\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa8\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xa9\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xaa\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xab\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xac\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xad\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xae\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xaf\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb0\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb1\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb2\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb3\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb4\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb5\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: \xb6\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb7\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb8\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xb9\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xba\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbb\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbc\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbd\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbe\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xbf\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc0\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc1\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc2\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc3\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc4\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc5\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc6\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc7\x99\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc8\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xc9\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xca\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcb\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,690	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcc\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcd\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xce\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xcf\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd0\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd1\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd2\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd3\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd4\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd5\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd6\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd7\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd8\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xd9\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xda\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdb\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdc\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdd\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xde\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xdf\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe0\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe1\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe2\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe3\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe4\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe5\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe6\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe7\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe8\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xe9\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xea\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xeb\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xec\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xed\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xee\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xef\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf0\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf1\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf2\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf3\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf4\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf5\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf6\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf7\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf8\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xf9\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \xfa\x99\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: `\xfb\x99\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`			
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\xfc\x99\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\xfd\x99\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\xfe\x99\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\xff\x99\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x00\x9a\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x01\x9a\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x02\x9a\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x03\x9a\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x04\x9a\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x05\x9a\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x06\x9a\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x07\x9a\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x08\x9a\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x9a\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x9a\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x0b\x9a\x00\x00\x00\x00\x00\x00` FileHandle: `0x000001c4`	success	`0x00000000`	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: `FilePositionInformation` HandleName: `C:\Users\Administrator\suoes.exe` FileInformation: `\x0c\x9a\x00\x00\x00\x00\x00\x00`	success	`0x00000000`	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x0e\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x0f\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x10\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x11\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x12\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x13\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x14\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x15\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x16\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x17\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x18\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x19\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1a\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1b\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1c\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1d\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,706	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1e\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x1f\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: !\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: "\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: #\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: $\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: %\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: &\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: '\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: (\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation:)\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: *\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: +\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ,\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: -\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: .\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a	**NtSetInformationFile**	FileInformationClass: FilePositionInformation	success	0x00000000	

		0x00000000		HandleName: C:\Users\Administrator\suoes.exe FileInformation: /\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 0\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 1\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 2\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 3\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 4\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 5\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 6\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 7\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 8\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: 9\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: :\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ;\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: <\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: =\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: >\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ?\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe	success	0x00000000	

				FileInformation: @\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4			
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: A\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: B\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: C\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: D\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: E\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: F\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: G\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: H\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: I\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: J\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: K\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: L\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: M\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: N\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: O\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: P\x9a\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Q\x9a\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000001c4			
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: R\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: S\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: T\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: U\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: V\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: W\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: X\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Y\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: Z\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: [\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: \\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation:]\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: ^\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: _\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: `\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: a\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: b\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	

2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: c\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: d\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtSetInformationFile**	FileInformationClass: FilePositionInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation: e\x9a\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,721	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,737	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:22,737	5280	0x00632d45 0x0040122a	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\suoes.exe DesiredAccess: FILE_WRITE_ATTRIBUTES|SYNCHRONIZE FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,737	5280	0x00632d45 0x0040122a	**NtSetInformationFile**	FileInformationClass: FileBasicInformation HandleName: C:\Users\Administrator\suoes.exe FileInformation:\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x87\x00\x00\x00\x00\x00\x00\x00 FileHandle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,737	5280	0x00632d45 0x0040122a	**NtClose**	Handle: 0x000001c4	success	0x00000000	
2019-04-18 21:18:22,737	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:22,737	5280	0x00632d40 0x0040122a	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:22,737	5280	0x00632d40 0x0040122a	**NtDelayExecution**	Milliseconds: 2000	success	0x00000000	
2019-04-18 21:18:24,753	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: shell32	success	0x00000000	
2019-04-18 21:18:24,753	5280	0x00632d59 0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x757ba000	success	0x00000000	
2019-04-18 21:18:24,753	5280	0x00632d59 0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x757ba000	success	0x00000000	
2019-04-18 21:18:24,753	5280	0x00632d59 0x0040122a	**NtOpenKeyEx**	ObjectAttributes:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\kiato.exe DesiredAccess: KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000000ec ObjectAttributesName:SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\kiato.exe	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,753	5280	0x00632d59 0x0040122a	**CoCreateInstance**	rclsid: 1F486A52-3CB1-48FD-8F50-B8DC300D9F9D ProgID: ClsContext: CLSCTX_INPROC_SERVER riid: ECF31D61-E474-453C-BEE7-DE68E441C6D0	success	0x00000000	1 time
2019-04-18 21:18:24,768	5280	0x00632d59 0x0040122a	**CoCreateInstance**	rclsid: 0E5AAE11-A475-4C5B-AB00-C66DE400274E ProgID: ClsContext: CLSCTX_INPROC_SERVER riid: ADD8BA80-002B-11D0-8F0F-00C04FD7D062	success	0x00000000	
2019-04-18 21:18:24,768	5280	0x00632d59 0x0040122a	**CoCreateInstance**	rclsid: 4DF0C730-DF9D-4AE3-9153-AA6B82E9795A ProgID: ClsContext: CLSCTX_INPROC_SERVER	success	0x00000000	

				riid: 8BE2D872-86AA-4D47-B776-32CCA40C7018			
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**DeviceIoControl**	DeviceHandle: 0x000001cc OutBuffer: \x14\x00\x00\x00#\x00\x00\xc0\xba\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 IoControlCode: 0x00470807 InBuffer: $\x00\x00\x00\x00\x00\x01\x00 c\xf5S\xbf\xb6\xd0\x11\x94\xf2\x00\xa0\xc9\x1e\xfb\x8b\x00\x00\x00\x00\x00\x00\x00\x00\x14\x00\x00\x00	success	0x00000001	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**DeviceIoControl**	DeviceHandle: 0x000001cc OutBuffer: \x14\x00\x00\x00\x00\x00\x00\xba\x02\x00\x00\x00\x00\x00\x00\\x00?\x00\\x00S\x00T\x00O\x00R\x00A \x00G\x00E\x00#\x00V\x00o\x001\x00u\x00m\x00e\x00#\x00{\x009\x008\x000\x006\x006\x006\x009\x003\x00- \x009\x00f\x005\x009\x00-\x001\x001\x00e\x008\x00-\x00a\x001\x001\x005\x00- \x008\x000\x006\x00e\x006\x00f\x006\x00e\x006\x009\x006\x003\x00}\x00#\x000\x000\x000\x000\x000\x000\x000\x000\x0 01\x00F\x005\x000\x000\x000\x000\x000\x00#\x00{\x005\x003\x00f\x005\x006\x003\x000\x00d\x00- \x00b\x006\x00b\x00f\x00-\x001\x001\x00d\x000\x00-\x009\x004\x00f\x002\x00- \x000\x000\x00a\x000\x00c\x009\x001\x00e\x00f\x00b\x008\x00b\x00}\x00\x00\x00\\x00\\x00?\x00\\x00I\x00D\x00 IoControlCode: 0x00470807 InBuffer: $\x00\x00\x00\x00\x00\x01\x00 c\xf5S\xbf\xb6\xd0\x11\x94\xf2\x00\xa0\xc9\x1e\xfb\x8b\x00\x00\x00\x00\x00\x00\x00\x00\x14\x00\x00\x00	success	0x00000001	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtDuplicateObject**	TargetHandle: 0x00000378 TargetProcessHandle: 0xffffffff Options: DUPLICATE_SAME_ACCESS SourceHandle: 0x00000380 SourceProcessHandle: 0xffffffff	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x00000380 Milliseconds: 1000	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\STORAGE#Volume#{98066693-9f59-11e8-a115-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2- 00a0c91efb8b} DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE FileHandle: 0x0000038c	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtClose**	Handle: 0x00000390	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtClose**	Handle: 0x0000038c	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\STORAGE#Volume#{98066693-9f59-11e8-a115-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2- 00a0c91efb8b} DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE FileHandle: 0x0000038c	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer: IoControlCode: IOCTL_MOUNTDEV_QUERY_DEVICE_NAME OutputBuffer: .\x00\\x00D\x00e\x00v\x00i\x00c\x00e\x00\\x00H\x00a\x00r\x00d\x00d\x00i\x00s\x00k\x00V\x00o\x00l\x00u\x 00m\x00e\x002\x00 FileHandle: 0x0000038c	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtClose**	Handle: 0x0000038c	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\MountPointManager DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x0000038c	success	0x00000000	

				FileAttributes: FILE_ATTRIBUTE_NORMAL			
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer:\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x18\x00\x00\x00.\x00\x00\x00\\x00D\x00e\ x00v\x00i\x00c\x00e\x00\\x00H\x00a\x00r\x00d\x00d\x00i\x00s\x00k\x00V\x00o\x00l\x00u\x00m\x00e\x002\x00 IoControlCode: IOCTL_MOUNTMGR_QUERY_POINTS OutputBuffer: FileHandle: 0x0000038c	failed	BUFFER_OVERFLOW	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer:\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x18\x00\x00\x00.\x00\x00\x00\\x00D\x00e\ x00v\x00i\x00c\x00e\x00\\x00H\x00a\x00r\x00d\x00d\x00i\x00s\x00k\x00V\x00o\x00l\x00u\x00m\x00e\x002\x00 IoControlCode: IOCTL_MOUNTMGR_QUERY_POINTS OutputBuffer:\xee\x00\x00\x00\x02\x00\x00\x00r\x00\x00\x00\x1c\x00\x00\x008\x00\x00\x00\x0c\x00\x00\x00D\x00\x00\x00 .\x00\x00\x00\x8e\x00\x00\x00`\x00\x00\x008\x00\x00\x00\x0c\x00\x00\x00D\x00\x00\x00.\x00\x00\x00\xdfc\xa1\xf1\x0 0\x00P\x1f\x00\x00\x00\x00\\x00D\x00e\x00v\x00i\x00c\x00e\x00\\x00H\x00a\x00r\x00d\x00d\x00i\x00s\x00k\x00V\x00o\ x00l\x00u\x00m\x00e\x002\x00\\x00D\x00o\x00s\x00D\x00e\x00v\x00i\x00c\x00e\x00s\x00\\x00C\x00:\x00\\x00?\x00?\x00 \\x00V\x00o\x00l\x00u\x00m\x00e\x00{\x00f\x001\x00a\x001\x006\x003\x00d\x00f\x00-\x000\x000\x000\x000\x00- \x000\x000\x000\x000\x00-\x000\x000\x000\x000\x00- \x005\x000\x001\x00f\x000\x000\x000\x000\x000\x000\x000\x000\x00}\x00 FileHandle: 0x0000038c	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtClose**	Handle: 0x0000038c	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x00000380	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume DesiredAccess: KEY_READ KeyHandle: 0x00000380 ObjectAttributesHandle: 0x00000288 ObjectAttributesName: Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtClose**	Handle: 0x00000378	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{f1a163d f-0000-0000-0000-501f00000000}\ DesiredAccess: KEY_READ KeyHandle: 0x0000038c ObjectAttributesHandle: 0x00000380 ObjectAttributesName: {f1a163df-0000-0000-0000-501f00000000}\	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x00000380	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{f1a163df- 0000-0000-0000-501f00000000}\Data KeyHandle: 0x0000038c ValueName: Data	failed	BUFFER_OVERFLOW	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtQueryValueKey**	Information: \xd6 \x00\x00 \xf0\xad\xbaA\x00\x00\x00\x08\x00\x00\x00\x00\x00\x00\x84\x00\x00\x00\x00\x00\x00\x000\x00\x00\x00\x00\x00\x00\x0 0\x00\xff\x06\xe7\x03\xff\x00\x00\x00\x16\x00\x00\x00j\x93\xeb\x9c\x1f\x00\x00\x00\x04@\x00\x00\x01\x00\x00\x00\x 00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\\x00\\x00?\x00\\x00S\x00T\x00O\x00R\x00A\x 00G\x00E\x00#\x00V\x00o\x00l\x00u\x00m\x00e\x00#\x00{\x009\x008\x000\x006\x006\x006\x009\x003\x00- \x009\x00f\x005\x009\x00-\x001\x001\x00e\x008\x00-\x00a\x001\x001\x005\x00- \x008\x000\x006\x00e\x006\x00f\x006\x00e\x006\x009\x006\x003\x00}\x00#\x000\x000\x000\x000\x000\x000\x000\x000\x0 01\x00F\x005\x000\x000\x000\x000\x000\x00#\x00{\x005\x003\x00f\x005\x006\x003\x000\x00d\x00- \x00b\x006\x00b\x00f\x00-\x001\x001\x00d\x000\x00-\x009\x004\x00f\x002\x00- \x000\x000\x00a\x000\x00c\x009\x001\x00e\x00f\x00b\x008\x00b\x00}\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x 00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0 0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x 00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 KeyHandle: 0x0000038c ValueName: Data Type: REG_BINARY FullName:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{f1a163df- 0000-0000-0000-501f00000000}\Data	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x0000038c	success	0x00000000	

2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume DesiredAccess: KEY_READ KeyHandle: 0x0000038c ObjectAttributesHandle: 0x00000288 ObjectAttributesName: Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{f1a163df-0000-0000-0000-501f00000000}\ DesiredAccess: KEY_READ KeyHandle: 0x00000380 ObjectAttributesHandle: 0x0000038c ObjectAttributesName: {f1a163df-0000-0000-0000-501f00000000}\	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x0000038c	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtQueryValueKey**	Information: 1 KeyHandle: 0x00000380 ValueName: Generation Type: REG_DWORD FullName:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{f1a163df-0000-0000-0000-501f00000000}\Generation	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x00000380	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtDuplicateObject**	TargetHandle: 0x0000038c TargetProcessHandle: 0xffffffff Options: DUPLICATE_SAME_ACCESS SourceHandle: 0x00000380 SourceProcessHandle: 0xffffffff	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x00000380 Milliseconds: 1000	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\IDE#CdRomQEMU_QEMU_DVD-ROM_____2.5+____#5&2770a7af&0&0.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b} DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE FileHandle: 0x00000390	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtClose**	Handle: 0x00000394	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtClose**	Handle: 0x00000390	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\IDE#CdRomQEMU_QEMU_DVD-ROM_____2.5+____#5&2770a7af&0&0.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b} DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE FileHandle: 0x00000390	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer: IoControlCode: IOCTL_MOUNTDEV_QUERY_DEVICE_NAME OutputBuffer: \x1c\x00\\x00D\x00e\x00v\x00i\x00c\x00e\x00\\x00C\x00d\x00R\x00o\x00m\x000\x00 FileHandle: 0x00000390	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtClose**	Handle: 0x00000390	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\MountPointManager DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x00000390 FileAttributes: FILE_ATTRIBUTE_NORMAL	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer:\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x18\x00\x00\x00\x1c\x00\x00\x00\\x00D\x00e\x00v\x00i\x00c\x00e\x00\\x00C\x00d\x00R\x00o\x00m\x000\x00 IoControlCode: IOCTL_MOUNTMGR_QUERY_POINTS OutputBuffer: FileHandle: 0x00000390	failed	BUFFER_OVERFLOW	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer:\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x18\x00\x00\x00\x1c\x00\x00\x00\\x00D\x00e\x00v\x00i\x00c\x00e\x00\\x00C\x00d\x00R\x00o\x00m\x000\x00 IoControlCode: IOCTL_MOUNTMGR_QUERY_POINTS	success	0x00000000	

				OutputBuffer: \xbe\x01\x00\x00\x02\x00\x00\x00B\x01\x00\x00`\x00\x00\x008\x00\x00\x00\xee\x00\x00\x00&\x01\x00\x00\x1 c\x00\x00\x00\xa2\x01\x00\x00\x1c\x00\x00\x008\x00\x00\x00\xee\x00\x00\x00&\x01\x00\x00\x1c\x00\x00\x00\\x00?\x00 ?\x00\\x00I\x00D\x00E\x00#\x00C\x00d\x00R\x00o\x00m\x00Q\x00E\x00M\x00U\x00_\x00Q\x00E\x00M\x00U\x00_\x00D\x00V\x 00D\x00- \x00R\x00O\x00M\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x0 0_\x00_\x00_\x00_\x002\x00.\x005\x00+\x00_\x00_\x00_\x00_\x00#\x005\x00&\x002\x007\x007\x000\x00a\x007\x00a\x00f\ x00&\x000\x00&\x000\x00.\x000\x00.\x000\x00#\x00{\x005\x003\x00f\x005\x006\x003\x000\x00d\x00- \x00b\x006\x00b\x00f\x00-\x001\x001\x00d\x000\x00 FileHandle: 0x00000390			
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtClose**	Handle: 0x00000390	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x00000380	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x0000038c	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume DesiredAccess: KEY_READ KeyHandle: 0x0000038c ObjectAttributesHandle: 0x00000288 ObjectAttributesName: Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{980666a 1-9f59-11e8-a115-806e6f6e6963}\ DesiredAccess: KEY_READ KeyHandle: 0x00000380 ObjectAttributesHandle: 0x0000038c ObjectAttributesName: {980666a1-9f59-11e8-a115-806e6f6e6963}\	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x0000038c	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{980666a1- 9f59-11e8-a115-806e6f6e6963}\Data KeyHandle: 0x00000380 ValueName: Data	failed	BUFFER_OVERFLOW	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtQueryValueKey**	Information: \xd6 \x00\x00 \xf0\xad\xba\x01\x00\x00\x00\x10\x00\x00\x00\x00\x00\x00\x80\xbd\xad\xdb\xba\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\xbd\xad\xdb\xba\xbd\xad\xdb\xba\xbd\xad\xdb\xba\xbd\xad\xdb\xba\x00\x00\x00\x00\x00\x00\x00\x00\x02\x 00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\\x00\\x00?\x00\\x00I\x00D\x00E \x00#\x00C\x00d\x00R\x00o\x00m\x00Q\x00E\x00M\x00U\x00_\x00Q\x00E\x00M\x00U\x00_\x00D\x00V\x00D\x00- \x00R\x00O\x00M\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x00_\x0 0_\x00_\x00_\x00_\x002\x00.\x005\x00+\x00_\x00_\x00_\x00_\x00#\x005\x00&\x002\x007\x007\x000\x00a\x007\x00a\x00f\ x00&\x000\x00&\x000\x00.\x000\x00.\x000\x00#\x00{\x005\x003\x00f\x005\x006\x003\x000\x00d\x00- \x00b\x006\x00b\x00f\x00-\x001\x001\x00d\x000\x00-\x009\x004\x00f\x002\x00- \x000\x000\x00a\x000\x00c\x009\x001\x00e\x00f\x00b\x008\x00b\x00}\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x 00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0 0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x 00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 KeyHandle: 0x00000380 ValueName: Data Type: REG_BINARY FullName:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{980666a1- 9f59-11e8-a115-806e6f6e6963}\Data	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x00000380	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume DesiredAccess: KEY_READ KeyHandle: 0x00000380 ObjectAttributesHandle: 0x00000288 ObjectAttributesName: Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{980666a 1-9f59-11e8-a115-806e6f6e6963}\ DesiredAccess: KEY_READ KeyHandle: 0x0000039c	success	0x00000000	

				ObjectAttributesHandle: 0x00000380 ObjectAttributesName: {980666a1-9f59-11e8-a115-806e6f6e6963}\			
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x00000380	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtQueryValueKey**	Information: 1 KeyHandle: 0x0000039c ValueName: Generation Type: REG_DWORD FullName:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{980666a1-9f59-11e8-a115-806e6f6e6963}\Generation	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x0000039c	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtDuplicateObject**	TargetHandle: 0x000003a4 TargetProcessHandle: 0xffffffff Options: DUPLICATE_SAME_ACCESS SourceHandle: 0x000003a0 SourceProcessHandle: 0xffffffff	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000003a0 Milliseconds: 1000	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\STORAGE#Volume#{98066693-9f59-11e8-a115-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b} DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE FileHandle: 0x000003b0	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtClose**	Handle: 0x000003b4	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtClose**	Handle: 0x000003b0	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\STORAGE#Volume#{98066693-9f59-11e8-a115-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b} DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE FileHandle: 0x000003b0	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer: IoControlCode: IOCTL_MOUNTDEV_QUERY_DEVICE_NAME OutputBuffer: .\x00\\x00D\x00e\x00v\x00i\x00c\x00e\x00\\x00H\x00a\x00r\x00d\x00d\x00i\x00s\x00k\x00V\x00o\x00l\x00u\x00m\x00e\x001\x00 FileHandle: 0x000003b0	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtClose**	Handle: 0x000003b0	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\MountPointManager DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x000003b0 FileAttributes: FILE_ATTRIBUTE_NORMAL	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer: \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x18\x00\x00\x00\x00.\x00\x00\x00\x00\\x00D\x00e\x00v\x00i\x00c\x00e\x00\\x00H\x00a\x00r\x00d\x00d\x00i\x00s\x00k\x00V\x00o\x00l\x00u\x00m\x00e\x001\x00 IoControlCode: IOCTL_MOUNTMGR_QUERY_POINTS OutputBuffer: FileHandle: 0x000003b0	failed	BUFFER_OVERFLOW	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer: \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x18\x00\x00\x00\x00.\x00\x00\x00\x00\\x00D\x00e\x00v\x00i\x00c\x00e\x00\\x00H\x00a\x00r\x00d\x00d\x00i\x00s\x00k\x00V\x00o\x00l\x00u\x00m\x00e\x001\x00 IoControlCode: IOCTL_MOUNTMGR_QUERY_POINTS OutputBuffer: \xba\x00\x00\x00\x01\x00\x00\x00Z\x00\x00\x00`\x00\x00\x00 \x00\x00\x00\x00\x0c\x00\x00\x00,\x00\x00\x00.\x00\x00\x00\xdfc\xa1\xf1\x00\x00\x10\x00\x00\x00\x00\x00\\x00D\x00e\x00v\x00i\x00c\x00e\x00\\x00H\x00a\x00r\x00d\x00d\x00i\x00s\x00k\x00V\x00o\x00l\x00u\x00m\x00e\x001\x00\\x00?\x00?\x00\\x00V\x00o\x001\x00u\x00m\x00e\x00{\x00f\x001\x00a\x001\x006\x003\x00d\x00f\x00-\x000\x000\x000\x000\x00- \x000\x000\x000\x000\x00-\x000\x000\x000\x000\x00- \x001\x000\x000\x000\x000\x000\x000\x000\x000\x000\x000\x000\x00}\x00 FileHandle: 0x000003b0	success	0x00000000	
2019-04-18 21:18:24,800	6812	0x00000000 0x00000000	**NtClose**	Handle: 0x000003b0	success	0x00000000	

2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x000003a0	success	0x00000000		
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x000003a4	success	0x00000000		
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume DesiredAccess: KEY_READ KeyHandle: 0x000003a4 ObjectAttributesHandle: 0x00000288 ObjectAttributesName: Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume	success	0x00000000		
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{f1a163df-0000-0000-0000-100000000000}\ DesiredAccess: KEY_READ KeyHandle: 0x000003a0 ObjectAttributesHandle: 0x000003a4 ObjectAttributesName: {f1a163df-0000-0000-0000-100000000000}\	success	0x00000000		
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x000003a4	success	0x00000000		
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{f1a163df-0000-0000-0000-100000000000}\Data KeyHandle: 0x000003a0 ValueName: Data	failed	BUFFER_OVERFLOW		
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtQueryValueKey**	Information: \xd6 \x00\x00 \xf0\xad\xba\x01\x00\x00\x00\x08\x00\x00\x00\x00\x00\x00\x84\x00\x00\x00\x00\x00\x00\x000\x00\x00\x00\x00\x00\x00 \x00\x00\xff\x06\xe7\x03\xff\x00\x00\x00\x16\x00\x00\x00z\x0b\xebV\x1e\x00\x00\x00\x04\x00\x00\x00\x01\x00\x00\x0 0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\\x00\\x00?\x00\\x00S\x00T\x00O\x00R\x00 A\x00G\x00E\x00#\x00V\x00o\x00l\x00u\x00m\x00e\x00#\x00{\x009\x008\x000\x006\x006\x006\x009\x003\x00- \x009\x00f\x005\x009\x00-\x001\x001\x00e\x008\x00-\x00a\x001\x001\x005\x00- \x008\x000\x006\x00e\x006\x00f\x006\x00e\x006\x009\x006\x003\x00}\x00#\x000\x000\x000\x000\x000\x000\x000\x000\x0 00\x000\x001\x000\x000\x000\x000\x000\x00#\x00{\x005\x003\x00f\x005\x006\x003\x000\x00d\x00- \x00b\x006\x00b\x00f\x00-\x001\x001\x00d\x000\x00-\x009\x004\x00f\x002\x00- \x000\x000\x00a\x000\x00c\x009\x001\x00e\x00f\x00b\x008\x00b\x00}\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x 00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0 0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x 00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 KeyHandle: 0x000003a0 ValueName: Data Type: REG_BINARY FullName:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{f1a163df-0000-0000-0000-100000000000}\Data	success	0x00000000		
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x000003a0	success	0x00000000		
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume DesiredAccess: KEY_READ KeyHandle: 0x000003a0 ObjectAttributesHandle: 0x00000288 ObjectAttributesName: Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume	success	0x00000000		
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{f1a163df-0000-0000-0000-100000000000}\ DesiredAccess: KEY_READ KeyHandle: 0x000003a4 ObjectAttributesHandle: 0x000003a0 ObjectAttributesName: {f1a163df-0000-0000-0000-100000000000}\	success	0x00000000		
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x000003a0	success	0x00000000		
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtQueryValueKey**	Information: 1 KeyHandle: 0x000003a4 ValueName: Generation Type: REG_DWORD FullName:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{f1a163df-0000-0000-0000-100000000000}\Generation	success	0x00000000		
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x000003a4	success	0x00000000		

2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\MountPointManager DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x000003a4 FileAttributes: FILE_ATTRIBUTE_NORMAL	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer: `\x00\\x00?\x00?\x00\\x00V\x00o\x001\x00u\x00m\x00e\x00{\x00f\x001\x00a\x001\x006\x003\x00d\x00f\x00- \x000\x000\x000\x000\x00-\x000\x000\x000\x000\x00-\x000\x000\x000\x000\x00- \x005\x000\x001\x00f\x000\x000\x000\x000\x000\x000\x000\x000\x00}\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x 00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0 0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\x00\x00\x00 IoControlCode: IOCTL_MOUNTMGR_QUERY_DOS_VOLUME_PATHS OutputBuffer: FileHandle: 0x000003a4	failed	BUFFER_OVERFLOW	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer: `\x00\\x00?\x00?\x00\\x00V\x00o\x001\x00u\x00m\x00e\x00{\x00f\x001\x00a\x001\x006\x003\x00d\x00f\x00- \x000\x000\x000\x000\x00-\x000\x000\x000\x000\x00-\x000\x000\x000\x000\x00- \x005\x000\x001\x00f\x000\x000\x000\x000\x000\x000\x000\x000\x00}\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x 00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0 0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\x00\x00\x00 IoControlCode: IOCTL_MOUNTMGR_QUERY_DOS_VOLUME_PATHS OutputBuffer: \x08\x00\x00\x00C\x00:\x00\x00\x00\x00\x00 FileHandle: 0x000003a4	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x000003a4	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\MountPointManager DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x000003a4 FileAttributes: FILE_ATTRIBUTE_NORMAL	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer: `\x00\\x00?\x00?\x00\\x00V\x00o\x001\x00u\x00m\x00e\x00{\x00f\x001\x00a\x001\x006\x003\x00d\x00f\x00- \x000\x000\x000\x000\x00-\x000\x000\x000\x000\x00-\x000\x000\x000\x000\x00- \x005\x000\x001\x00f\x000\x000\x000\x000\x000\x000\x000\x000\x00}\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x 00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0 0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\x00\x00\x00 IoControlCode: IOCTL_MOUNTMGR_QUERY_DOS_VOLUME_PATHS OutputBuffer: FileHandle: 0x000003a4	failed	BUFFER_OVERFLOW	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer: `\x00\\x00?\x00?\x00\\x00V\x00o\x001\x00u\x00m\x00e\x00{\x00f\x001\x00a\x001\x006\x003\x00d\x00f\x00- \x000\x000\x000\x000\x00-\x000\x000\x000\x000\x00-\x000\x000\x000\x000\x00- \x005\x000\x001\x00f\x000\x000\x000\x000\x000\x000\x000\x000\x00}\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x 00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0 0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ x00\x00\x00\x00\x00\x00 IoControlCode: IOCTL_MOUNTMGR_QUERY_DOS_VOLUME_PATHS OutputBuffer: \x08\x00\x00\x00C\x00:\x00\x00\x00\x00\x00 FileHandle: 0x000003a4	success	0x00000000	
2019-04-18 21:18:24,800	1488	0x00000000 0x00000000	**NtClose**	Handle: 0x000003a4	success	0x00000000	1 time
2019-04-18 21:18:24,800	1488	0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE	success	0x00000000	

<table>
<tr><td></td><td></td><td>0x00000000</td><td></td><td>FileName: \??\MountPointManager
DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE
ExistedBefore: yes
StackPivoted: no
CreateDisposition: FILE_OPEN
FileHandle: 0x000003a4
FileAttributes: FILE_ATTRIBUTE_NORMAL</td><td></td><td></td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>1488</td><td>0x00000000
0x00000000</td><td>NtDeviceIoControlFile</td><td>InputBuffer: `\x00\\x00?\x00?\x00\\x00V\x00o\x00l\x00u\x00m\x00e\x00{\x009\x008\x000\x006\x006\x006\x00a\x001\x00-\x009\x00f\x005\x009\x00-\x001\x001\x00e\x008\x00-\x00a\x001\x001\x005\x00-\x008\x000\x006\x00e\x006\x00f\x006\x00e\x006\x009\x006\x003\x00}\x00
IoControlCode: IOCTL_MOUNTMGR_QUERY_DOS_VOLUME_PATHS
OutputBuffer:
FileHandle: 0x000003a4</td><td>failed</td><td>BUFFER_OVERFLOW</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>1488</td><td>0x00000000
0x00000000</td><td>NtDeviceIoControlFile</td><td>InputBuffer: `\x00\\x00?\x00?\x00\\x00V\x00o\x00l\x00u\x00m\x00e\x00{\x009\x008\x000\x006\x006\x006\x00a\x001\x00-\x009\x00f\x005\x009\x00-\x001\x001\x00e\x008\x00-\x00a\x001\x001\x005\x00-\x008\x000\x006\x00e\x006\x00f\x006\x00e\x006\x009\x006\x003\x00}\x00
IoControlCode: IOCTL_MOUNTMGR_QUERY_DOS_VOLUME_PATHS
OutputBuffer: \x08\x00\x00\x00D\x00:\x00\x00\x00\x00\x00
FileHandle: 0x000003a4</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>1488</td><td>0x00000000
0x00000000</td><td>NtClose</td><td>Handle: 0x000003a4</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>1488</td><td>0x00000000
0x00000000</td><td>NtCreateFile</td><td>ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE
FileName: \??\MountPointManager
DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE
ExistedBefore: yes
StackPivoted: no
CreateDisposition: FILE_OPEN
FileHandle: 0x000003a4
FileAttributes: FILE_ATTRIBUTE_NORMAL</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>1488</td><td>0x00000000
0x00000000</td><td>NtDeviceIoControlFile</td><td>InputBuffer: `\x00\\x00?\x00?\x00\\x00V\x00o\x00l\x00u\x00m\x00e\x00{\x009\x008\x000\x006\x006\x006\x00a\x001\x00-\x009\x00f\x005\x009\x00-\x001\x001\x00e\x008\x00-\x00a\x001\x001\x005\x00-\x008\x000\x006\x00e\x006\x00f\x006\x00e\x006\x009\x006\x003\x00}\x00
IoControlCode: IOCTL_MOUNTMGR_QUERY_DOS_VOLUME_PATHS
OutputBuffer:
FileHandle: 0x000003a4</td><td>failed</td><td>BUFFER_OVERFLOW</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>1488</td><td>0x00000000
0x00000000</td><td>NtDeviceIoControlFile</td><td>InputBuffer: `\x00\\x00?\x00?\x00\\x00V\x00o\x00l\x00u\x00m\x00e\x00{\x009\x008\x000\x006\x006\x006\x00a\x001\x00-\x009\x00f\x005\x009\x00-\x001\x001\x00e\x008\x00-\x00a\x001\x001\x005\x00-\x008\x000\x006\x00e\x006\x00f\x006\x00e\x006\x009\x006\x003\x00}\x00
IoControlCode: IOCTL_MOUNTMGR_QUERY_DOS_VOLUME_PATHS
OutputBuffer: \x08\x00\x00\x00D\x00:\x00\x00\x00\x00\x00
FileHandle: 0x000003a4</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>1488</td><td>0x00000000
0x00000000</td><td>NtClose</td><td>Handle: 0x000003a4</td><td>success</td><td>0x00000000</td><td>1 time</td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>1488</td><td>0x00000000
0x00000000</td><td>NtCreateFile</td><td>ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE
FileName: \??\MountPointManager</td><td>success</td><td>0x00000000</td><td></td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td></td><td>DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE
ExistedBefore: yes
StackPivoted: no
CreateDisposition: FILE_OPEN
FileHandle: 0x000003a4
FileAttributes: FILE_ATTRIBUTE_NORMAL</td><td></td><td></td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>1488</td><td>0x00000000
0x00000000</td><td>NtDeviceIoControlFile</td><td>InputBuffer: `\x00\\x00?\x00?\x00\\x00V\x00o\x00l\x00u\x00m\x00e\x00{\x00f\x001\x00a\x001\x006\x003\x00d\x00f\x00-
\x000\x000\x000\x000\x00-\x000\x000\x000\x000\x00-\x000\x000\x000\x000\x00-
\x001\x000\x000\x000\x000\x000\x000\x000\x000\x000\x000\x000\x00}\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00

IoControlCode: IOCTL_MOUNTMGR_QUERY_DOS_VOLUME_PATHS
OutputBuffer: \x02\x00\x00\x00\x00\x00
FileHandle: 0x000003a4</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>1488</td><td>0x00000000
0x00000000</td><td>NtClose</td><td>Handle: 0x000003a4</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>1488</td><td>0x00000000
0x00000000</td><td>NtCreateFile</td><td>ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE
FileName: \??\MountPointManager
DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE
ExistedBefore: yes
StackPivoted: no
CreateDisposition: FILE_OPEN
FileHandle: 0x000003a4
FileAttributes: FILE_ATTRIBUTE_NORMAL</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>1488</td><td>0x00000000
0x00000000</td><td>NtDeviceIoControlFile</td><td>InputBuffer: `\x00\\x00?\x00?\x00\\x00V\x00o\x00l\x00u\x00m\x00e\x00{\x00f\x001\x00a\x001\x006\x003\x00d\x00f\x00-
\x000\x000\x000\x000\x00-\x000\x000\x000\x000\x00-\x000\x000\x000\x000\x00-
\x001\x000\x000\x000\x000\x000\x000\x000\x000\x000\x000\x000\x00}\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00

IoControlCode: IOCTL_MOUNTMGR_QUERY_DOS_VOLUME_PATHS
OutputBuffer: \x02\x00\x00\x00\x00\x00
FileHandle: 0x000003a4</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>1488</td><td>0x00000000
0x00000000</td><td>NtClose</td><td>Handle: 0x000003a4</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>5280</td><td>0x00632d59
0x0040122a</td><td>CoCreateInstance</td><td>rclsid: 00000323-0000-0000-C000-000000000046
ProgID:
ClsContext: CLSCTX_INPROC_SERVER
riid: 00000146-0000-0000-C000-000000000046</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>828</td><td>0x00000000
0x00000000</td><td>NtDuplicateObject</td><td>TargetHandle: 0x000003f0
TargetProcessHandle: 0xffffffff
Options: DUPLICATE_SAME_ACCESS
SourceHandle: 0xfffffffe
SourceProcessHandle: 0xffffffff</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>1552</td><td>0x00000000
0x00000000</td><td>NtSetTimerEx</td><td>Status: Skipped
Milliseconds: 60000</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>7476</td><td>0x00000000
0x00000000</td><td>NtProtectVirtualMemory</td><td>StackPivoted: no
OldAccessProtection: PAGE_READONLY
NumberOfBytesProtected: 0x00001000
NewAccessProtection: PAGE_READWRITE
MemoryType: 0x01000000
ProcessHandle: 0xffffffff
BaseAddress: 0x726d7000</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>7476</td><td>0x00000000
0x00000000</td><td>NtProtectVirtualMemory</td><td>StackPivoted: no
OldAccessProtection: PAGE_READWRITE
NumberOfBytesProtected: 0x00001000
NewAccessProtection: PAGE_READONLY
MemoryType: 0x01000000
ProcessHandle: 0xffffffff
BaseAddress: 0x726d7000</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>7476</td><td>0x00000000
0x00000000</td><td>NtProtectVirtualMemory</td><td>StackPivoted: no
OldAccessProtection: PAGE_READONLY</td><td>success</td><td>0x00000000</td><td></td></tr>
</table>

				NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x726d7000			
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x726d7000	success	0x00000000	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x726d7000	success	0x00000000	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x726d7000	success	0x00000000	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtOpenKey**	ObjectAttributes: HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsRuntime DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED KeyHandle: 0x00000428 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\MACHINE\Software\Microsoft\WindowsRuntime	success	0x00000000	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtOpenKey**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED KeyHandle: 0x0000042c ObjectAttributesHandle: 0x00000428 ObjectAttributesName: ActivatableClassId	success	0x00000000	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtOpenKey**	ObjectAttributes:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.FileTypeAssociation DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED KeyHandle: 0x00000430 ObjectAttributesHandle: 0x0000042c ObjectAttributesName: Windows.Internal.StateRepository.FileTypeAssociation	success	0x00000000	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 0 KeyHandle: 0x00000430	success	0x00000000	

				KeyInformation:\xef\xbf\xa3B\\xef\xbe\x9e\xef\xbf\x9b3\xef\xbf\x94\x01\x00\x00\x00\x00h\x00\x00\x00W\x00i\x00n\x00d\x00o\x00w\x00s\x00.\x00I\x00n\x00t\x00e\x00r\x00n\x00a\x00l\x00.\x00S\x00t\x00a\x00t\x00e\x00R\x00e\x00p\x00o\x00s\x00i\x00t\x00o\x00r\x00y\x00.\x00F\x00i\x00l\x00e\x00T\x00y\x00p\x00e\x00A\x00s\x00s\x00o\x00c\x00i\x00a\x00t\x00i\x00o\x00n\x00\x02\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00(\xef\xbf\x80f\x00\xef\xbe\xb5\x04\x00\x00l\xef\xbf\xb6\xef\xbf\x99\x04\xef\xbf\xaeGuw\x18\xef\xbf\xaeb\x00\xef\xbf\xaeGuw\x00\x00\x00\x00\x00\x00\x00\x00`\x0ef\x00`\x0ef\x00\xef\xbf\x80\x00^\x00\xef\xbf\xa0\xef\xbf\xb7\xef\xbf\x99\x04\xef\xbe\x8dc\xef\xbf\xa8t\xef\xbf\xa0\xef\xbf\xb7\xef\xbf\x99\x04\xef\xbe\x9c\xef\xbf\xb6\xef\xbf\x99\x04-c[n\x07\x00\x00\x00;\x00\x00\x00\x00\x00\x00\x00\x00\x00\xef\xbf\xb0\xef\xbf\x99\x04h\xef\xbe\xbdd\x004\x00\x00\xef\xbf\x80\x00\x00\x00\x00\xef\xbe\xa8\xef\xbf\xb6\xef\xbf\x99\x04\xef\xbe\xb9`[n\x00\x00\x00\x00\xef\xbf\x8c\xef\xbf\xb6\xef\xbf\x99\x04-c[n\x07\x00\x00\x00=\x00\x00\x00\x00\x00\x00\x00\x00\xef\xbf\xa0\xef\xbf\x99\x04\xef\xbf\x8c\xef\xbf\xbf\xef\xbf\x99\x04\x00\x00\x00\x00\x00\x00\x00\xef\xbf\x98\xef\xbf\xb6\xef\xbf\x99\x04\xef\xbe\xb9`[n\x00\x00\x00\x00\xef\xbf\xbc\xef\xbf\xb6\xef\xbf\x99\x04\xef\xbe\x86s[n\x00\x00\x00\x00\xef\xbe\x91LX\xef\xbf\xb90\xef\xbf\xb2\xef\xbf\x99\x04x\xef\xbf\xb7\xef\xbf\x93\x02\xef\xbf\x8c\xef\xbf\xbf\xef\xbf\x99\x04\xef\xbe\x80]]n m\xef\xbf\x9e\xef\xbe\x93\xef\xbf\xbe\xef\xbf\xbf\xef\xbf\xbf\xef\xbf\xbfL\xef\xbf\xb7\xef\xbf\x99\x04mI\n$\x00\x00\x00\xef\xbf\x88\xef\xbe\xa0_n<\xef\xbe\xa5_n\x01\x00\x00\x00\x00\x00\x00\x005\xef\xbe\xa5_nX\xef\xbe\xa4_n\xef\xbf\xa8\x14b\x00\x1d~'z(\x04\x00\x00\xef\xbf\xa0\x14b\x00\xef\xbf\xa8\x14b\x00\xef\xbf\xa8\xef\xbe\xa4_n(\xef\xbf\xb7\xef\xbf\x99\x048~_n\xef\xbf\x8c\xef\xbf\xbf\xef\xbf\x99\x04\x10%xwQ{~ \xef\xbf\xbe\xef\xbf\xbf\xef\xbf\xbf\xef\xbf\xbf\xef\xbe\x88\xef\xbf\xb7\xef\xbf\x99\x04\xef\xbe\x85\xef\xbe\x84\xef\xbf\xb0t\x00\x00\x00\x00(\x04\x00\x00\xef\xbf\xa0\x14b\x00\xef\xbf\xa8\x14b\x00\xef\xbf\xa8\xef\xbe\xbef\x00\x18\x00\x00\x00(\x04\x00\x00\xef\xbe\xa4\xef\xbf\xb7\xef\xbf\x99\x04@\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xef\xbe\xbc\xef\xbf\xb7\xef\xbf\x99\x04#R\xef\xbf\xa8t\x19\x01\x02\x00\xef\xbf\xa8\x14b\x00\x00\xef\xbf\xb4\xef\xbf\xb0t\xef\xbf\xa0\x14b\x00OR\xef\xbf\xa8t$\x00&\x00\x10\x19e\x00\x00\x00\x00\x00`\x0ef\x00\xef\xbe\xb07\xef\xbf\xb1t\xef\xbf\x86\xef\xbe\xa1\xef\xbe\x9f\xef\xbf\xa1\xef\xbf\x90\xef\xbf\xb7\xef\xbf\x99\x04\x1c\xef\xbf\xb4\xef\xbf\xb0t\xef\xbf\xad\xef\xbf\xb3\xef\xbf\xb0t			
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: 1 KeyHandle: 0x00000430 ValueName: ActivationType Type: REG_DWORD FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.FileTypeAssociation\ActivationType	success	0x00000000	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: StateRepository KeyHandle: 0x00000430 ValueName: Server Type: REG_SZ FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.FileTypeAssociation\Server	success	0x00000000	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.FileTypeAssociation\DllPath KeyHandle: 0x00000430 ValueName: DllPath	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.FileTypeAssociation\Threading KeyHandle: 0x00000430 ValueName: Threading	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: 0 KeyHandle: 0x00000430 ValueName: TrustLevel Type: REG_DWORD FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.FileTypeAssociation\TrustLevel	success	0x00000000	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.FileTypeAssociation\CustomAttributes DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000430 ObjectAttributesName: CustomAttributes	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.FileTypeAssociation\RemoteServer KeyHandle: 0x00000430 ValueName: RemoteServer	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.FileTypeAssociation\ActivateAsUser KeyHandle: 0x00000430 ValueName: ActivateAsUser	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,800	7476	0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.FileTypeAssociation\ActivateInSharedBroker	failed	OBJECT_NAME_NOT_FOUND	

<table>
<tr><td></td><td></td><td>0x00000000</td><td></td><td>KeyHandle: 0x00000430
ValueName: ActivateInSharedBroker</td><td></td><td></td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>7476</td><td>0x00000000
0x00000000</td><td>NtQueryValueKey</td><td>FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.FileTypeAssociation\Permissions
KeyHandle: 0x00000430
ValueName: Permissions</td><td>failed</td><td>OBJECT_NAME_NOT_FOUND</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>7476</td><td>0x00000000
0x00000000</td><td>NtOpenKeyEx</td><td>ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\Diagnosis
DesiredAccess: KEY_READ
KeyHandle: 0x00000000
ObjectAttributesHandle: 0x000000ec
ObjectAttributesName: SOFTWARE\Microsoft\OLE\Diagnosis</td><td>failed</td><td>OBJECT_NAME_NOT_FOUND</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>7476</td><td>0x00000000
0x00000000</td><td>NtOpenKey</td><td>ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\Server
DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED
KeyHandle: 0x00000434
ObjectAttributesHandle: 0x00000428
ObjectAttributesName: Server</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>7476</td><td>0x00000000
0x00000000</td><td>NtOpenKey</td><td>ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\Server\StateRepository
DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED
KeyHandle: 0x00000438
ObjectAttributesHandle: 0x00000434
ObjectAttributesName: StateRepository</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>7476</td><td>0x00000000
0x00000000</td><td>NtQueryKey</td><td>KeyInformationClass: 0
KeyHandle: 0x00000438
KeyInformation:\xef\xbe\xbb\xef\xbe\xb3(=\xef\xbf\xae\xef\xbf\x91\xef\xbf\x93\x01\x00\x00\x00\x00\x1e\x00\x00\x00S\x00t\x00a\x00t\x00e\x00R\x00e\x00p\x00o\x00s\x00i\x00t\x00o\x00r\x00y\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xef\xbe\xae\x00\x00\x00\x00\x00`\xef\xbf\xb1\xef\xbf\x89\x04\x00\x00\x00\x00\x00\x00\xef\xbe\xa6\x00\x00\x00\x00\x00p\xef\xbf\xb1\xef\xbf\x89\x04\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xef\xbe\x8e\x00\x00\x00\x00\x00\xef\xbe\xa0\xef\xbf\xb1\xef\xbf\x89\x04\x00\x00\x00\x00\\x00R\x00E\x00G\x00I\x00S\x00T\x00R\x00\x00\x00~\x00M\x00A\x00\xef\xbf\x80\xef\xbf\xb1\xef\xbf\x89\x04\x00\x00\x00\x00E\x00\\x00S\x00O\x00F\x00T\x00W\x00A\x00R\x00E\x00\\x00M\x00i\x00c\x00r\x00o\x00s\x00o\x00f\x00t\x00\\x00W\x00i\x00n\x00d\x00o\x00w\x00s\x00R\x00u\x00n\x00t\x00i\x00m\x00e\x00\\x00A\x00c\x00t\x00i\x00\xef\xbe\x94\x00\xef\xbe\x94\x00t\x00a\x00
\xef\xbf\xb2\xef\xbf\x89\x04\x00\x00\x00\x00\\x00R\x00E\x00G\x00I\x00S\x00T\x00R\x00Y\x00\\x00M\x00A\x00C\x00H\x00I\x00N\x00E\x00\\x00S\x00O\x00F\x00T\x00W\x00A\x00R\x00E\x00\\x00M\x00i\x00c\x00r\x00o\x00s\x00o\x00f\x00t\x00\\x00W\x00i\x00n\x00d\x00o\x00w\x00s\x00R\x00u\x00n\x00t\x00i\x00m\x00e\x00\\x00S\x00e\x00r\x00v\x00e\x00r\x00\\x00S\x00t\x00a\x00t\x00e\x00R\x00e\x00p\x00o\x00s\x00i\x00t\x00o\x00r\x00y\x00e\x00s\x00I\x00d\x00\x00\x00\x00\x00\x1e\x00
\x00\x00\x00\x00\x00\xef\xbf\x90\x16e\x00\x00\x00\x00\x000\x00\x00\x00\x00\x00\x00\x004\x04\x00\x00\x00\x00\x00\x00\xef\xbf\x80\xef\xbf\xb2\xef\xbf\x89\x04\x00\x00\x00\x00@\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>7476</td><td>0x00000000
0x00000000</td><td>NtOpenKey</td><td>ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\DebugInformation
DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED
KeyHandle: 0x00000000
ObjectAttributesHandle: 0x00000428
ObjectAttributesName: DebugInformation</td><td>failed</td><td>OBJECT_NAME_NOT_FOUND</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>7476</td><td>0x00000000
0x00000000</td><td>NtQueryValueKey</td><td>FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\Server\StateRepository\ExePath
KeyHandle: 0x00000438
ValueName: ExePath</td><td>failed</td><td>OBJECT_NAME_NOT_FOUND</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>7476</td><td>0x00000000
0x00000000</td><td>NtQueryValueKey</td><td>FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\Server\StateRepository\CommandLine
KeyHandle: 0x00000438
ValueName: CommandLine</td><td>failed</td><td>OBJECT_NAME_NOT_FOUND</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>7476</td><td>0x00000000
0x00000000</td><td>NtQueryValueKey</td><td>Information: 1
KeyHandle: 0x00000438
ValueName: IdentityType
Type: REG_DWORD
FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\Server\StateRepository\IdentityType</td><td>success</td><td>0x00000000</td><td></td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>7476</td><td>0x00000000
0x00000000</td><td>NtQueryValueKey</td><td>FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\Server\StateRepository\Permissions
KeyHandle: 0x00000438
ValueName: Permissions</td><td>failed</td><td>BUFFER_OVERFLOW</td><td>1 time</td></tr>
<tr><td>2019-04-18 21:18:24,800</td><td>7476</td><td>0x00000000</td><td>NtQueryValueKey</td><td>Information:\x01\x00\x14\x80\x9c\x00\x00\x00\xa8\x00\x00\x00\x14\x00\x00\x000\x00\x00\x00\x02\x00\x1c\x00\x01\x00\x00\x00\x11\x00\x14\x00\x04\x00\x00\x00\x01\x01\x00\x00\x00\x00\x00\x10\x00\x10\x00\x00\x02\x001\x00\x03\x00\x00\x00\x00\x00\x14\x00\x1f\x00\x00\x00\x01\x01\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x18\x00\x1f\x00\x00\x00\x01\x02\x00\x00\x00\x00\x00\x0f\x02\x00\x00\x00\x01\x00\x00\x00\x00\x008\x00\x1f\x00\x00\x00\x01
\x00\x00\x00\x00\x00\x0f\x03\x00\x00\x00\x00\x04\x00\x00\xceJ\x93Y\xb9\xcf\x0buu\xc0\xf2\x9b\xb2\xb4\xc2\x98\xd4F
\xdd\xf9\x02z\x87\xec\x14e\x11w\xd6\xe9\x96U\x01\x01\x00\x00\x00\x00\x00\x05
\x00\x00\x00\x01\x02\x00\x00\x00\x00\x00\x05 \x00\x00\x00!\x02\x00\x00</td><td>success</td><td>0x00000000</td><td></td></tr>
</table>

		0x00000000		KeyHandle: 0x00000438 ValueName: Permissions Type: REG_BINARY FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\Server\StateRepository\Permissions			
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\Server\StateRepository\ActivatableClasses KeyHandle: 0x00000438 ValueName: ActivatableClasses	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: 2 KeyHandle: 0x00000438 ValueName: ServerType Type: REG_DWORD FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\Server\StateRepository\ServerType	success	0x00000000	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtQueryValueKey**	FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\Server\StateRepository\AppId KeyHandle: 0x00000438 ValueName: AppId	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: nt authority\system KeyHandle: 0x00000438 ValueName: Identity Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\Server\StateRepository\Identity	success	0x00000000	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: StateRepository KeyHandle: 0x00000438 ValueName: ServiceName Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\Server\StateRepository\ServiceName	success	0x00000000	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\Server\StateRepository\ExplicitPsmActivationType KeyHandle: 0x00000438 ValueName: ExplicitPsmActivationType	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,800	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\Server\StateRepository\CustomAttributes DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000438 ObjectAttributesName: CustomAttributes	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x00000438	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x00000430	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtDuplicateObject**	TargetHandle: 0x0000043c TargetProcessHandle: 0xffffffff Options: DUPLICATE_SAME_ACCESS SourceHandle: 0xfffffffe SourceProcessHandle: 0xffffffff	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQuerySystemTime**		success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x74df0000 FileName: combase.dll	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtDuplicateObject**	TargetHandle: 0x00000414 TargetProcessHandle: 0xffffffff Options: DUPLICATE_SAME_ACCESS SourceHandle: 0xfffffffe SourceProcessHandle: 0xffffffff	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**CoCreateInstance**	rclsid: 0000032A-0000-0000-C000-000000000046 ProgID: ClsContext: CLSCTX_INPROC_SERVER riid: 00000149-0000-0000-C000-000000000046	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**CoCreateInstance**	rclsid: 00000339-0000-0000-C000-000000000046 ProgID: ClsContext: CLSCTX_NO_CODE_DOWNLOAD|CLSCTX_INPROC_HANDLER|CLSCTX_INPROC_SERVER riid: 00000003-0000-0000-C000-000000000046	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000002c6 KeyInformation: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000002c6 KeyInformation: \x01\x00\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Interface\{8645456F-D9A2-4B82-AFEC-58F0E8DF0ACF} DesiredAccess: KEY_READ	failed	OBJECT_NAME_NOT_FOUND	

				KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000002c6 ObjectAttributesName: Interface\{8645456F-D9A2-4B82-AFEC-58F0E8DF0ACF}			
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\Software\Classes\Interface\{8645456F-D9A2-4B82-AFEC-58F0E8DF0ACF} DesiredAccess: KEY_READ KeyHandle: 0x00000418 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \Registry\Machine\Software\Classes\Interface\{8645456F-D9A2-4B82-AFEC-58F0E8DF0ACF}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{8645456f-d9a2-4b82-afec-58f0e8df0acf}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{8645456f-d9a2-4b82-afec-58f0e8df0acf}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\Interface\{8645456f-d9a2-4b82-afec-58f0e8df0acf}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{8645456f-d9a2-4b82-afec-58f0e8df0acf}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x00000444 ObjectAttributesHandle: 0x0000041a ObjectAttributesName: ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x00000446 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{8645456f-d9a2-4b82-afec-58f0e8df0acf}\ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x00000446 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{8645456f-d9a2-4b82-afec-58f0e8df0acf}\ProxyStubClsid32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\Interface\{8645456f-d9a2-4b82-afec-58f0e8df0acf}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: {c53e07ec-25f3-4093-aa39-fc67ea22e99d} KeyHandle: 0x00000446 ValueName: Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{8645456f-d9a2-4b82-afec-58f0e8df0acf}\ProxyStubClsid32\(Default)	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x00000446	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x0000041a	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000002a2 KeyInformation: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000002a2 KeyInformation: \x01\x00\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D} DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000002a2 ObjectAttributesName: CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D} DesiredAccess: KEY_READ KeyHandle: 0x00000418 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \Registry\Machine\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000	**NtQueryKey**	KeyInformationClass: 3	success	0x00000000	

		0x00000000		KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}			
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\TreatAs DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\TreatAs	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\TreatAs DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x0000041a ObjectAttributesName: TreatAs	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	1 time
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d} DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\(Default) KeyHandle: 0x0000041a ValueName:	failed	BUFFER_OVERFLOW	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d} DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: PSFactoryBuffer KeyHandle: 0x0000041a ValueName: Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\(Default)	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocServer32 DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocServer32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocServer32 DesiredAccess: KEY_READ KeyHandle: 0x00000444	success	0x00000000	

				ObjectAttributesHandle: 0x0000041a ObjectAttributesName: InprocServer32			
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x00000446 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x00000446 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32\InprocServer32 KeyHandle: 0x00000446 ValueName: InprocServer32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x00000446 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x00000446 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32\(Default) KeyHandle: 0x00000446 ValueName:	failed	BUFFER_OVERFLOW	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x00000446 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x00000446 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: C:\Windows\SysWOW64\\Windows.StateRepositoryPS.dll KeyHandle: 0x00000446 ValueName: Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32\(Default)	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x00000446 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x00000446 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000	failed	OBJECT_NAME_NOT_FOUND	

				ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32			
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: Both KeyHandle: 0x00000446 ValueName: ThreadingModel Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32\ThreadingModel	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x00000446	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocHandler32 DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocHandler32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocHandler32 DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x0000041a ObjectAttributesName: InprocHandler32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocHandler DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocHandler	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocHandler DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x0000041a ObjectAttributesName: InprocHandler	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x0000041a	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000002a2 KeyInformation: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000002a2 KeyInformation: \x01\x00\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D} DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000002a2 ObjectAttributesName: CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D} DesiredAccess: KEY_READ KeyHandle: 0x00000418	success	0x00000000	

				ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \Registry\Machine\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D}			
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\TreatAs DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\TreatAs	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\TreatAs DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x0000041a ObjectAttributesName: TreatAs	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	1 time
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d} DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\(Default) KeyHandle: 0x0000041a ValueName:	failed	BUFFER_OVERFLOW	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d} DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: PSFactoryBuffer KeyHandle: 0x0000041a ValueName: Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\(Default)	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocServer32 DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocServer32	failed	OBJECT_NAME_NOT_FOUND	

2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocServer32 DesiredAccess: KEY_READ KeyHandle: 0x00000444 ObjectAttributesHandle: 0x0000041a ObjectAttributesName: InprocServer32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x00000446 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x00000446 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32\InprocServer32 KeyHandle: 0x00000446 ValueName: InprocServer32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x00000446 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x00000446 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32\(Default) KeyHandle: 0x00000446 ValueName:	failed	BUFFER_OVERFLOW	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x00000446 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x00000446 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: C:\Windows\SysWOW64\\Windows.StateRepositoryPS.dll KeyHandle: 0x00000446 ValueName: Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32\(Default)	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x00000446 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x00000446 KeyInformation: \x01\x04\x00\x00	success	0x00000000	

2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: Both KeyHandle: 0x00000446 ValueName: ThreadingModel Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32\ThreadingModel	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x00000446	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocHandler32 DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocHandler32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocHandler32 DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x0000041a ObjectAttributesName: InprocHandler32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocHandler DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocHandler	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocHandler DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x0000041a ObjectAttributesName: InprocHandler	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\LocalServer32 DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\LocalServer32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\LocalServer32 DesiredAccess: KEY_READ	failed	OBJECT_NAME_NOT_FOUND	

				KeyHandle: 0x00000000 ObjectAttributesHandle: 0x0000041a ObjectAttributesName: LocalServer32			
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d} DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\AppID KeyHandle: 0x0000041a ValueName: AppID	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\LocalServer DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\LocalServer	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\LocalServer DesiredAccess: KEY_QUERY_VALUE KeyHandle: 0x00000000 ObjectAttributesHandle: 0x0000041a ObjectAttributesName: LocalServer	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000002a2 KeyInformation: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000002a2 KeyInformation: \x01\x00\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D} DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000002a2 ObjectAttributesName: CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D} DesiredAccess: KEY_READ KeyHandle: 0x00000444 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \Registry\Machine\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x00000446 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x00000446 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\Elevation DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\Elevation	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\Elevation	failed	OBJECT_NAME_NOT_FOUND	

		0x00000000		DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000446 ObjectAttributesName: Elevation			
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x00000446	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x0000041a	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000002c6 KeyInformation: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000002c6 KeyInformation: \x01\x00\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D} DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000002c6 ObjectAttributesName: CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D} DesiredAccess: KEY_READ KeyHandle: 0x00000418 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \Registry\Machine\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\TreatAs DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\TreatAs	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\TreatAs DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x0000041a ObjectAttributesName: TreatAs	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x0000041a	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: C:\Windows\SysWOW64\Windows.StateRepositoryPS.dll	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000002c6 KeyInformation: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000002c6 KeyInformation: \x01\x00\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Interface\{AF86E2E0-B12D-4C6A-9C5A-D7AA65101E90} DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000002c6 ObjectAttributesName: Interface\{AF86E2E0-B12D-4C6A-9C5A-D7AA65101E90}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\Software\Classes\Interface\{AF86E2E0-B12D-4C6A-9C5A-D7AA65101E90}	success	0x00000000	

		0x00000000		DesiredAccess: KEY_READ KeyHandle: 0x00000418 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \Registry\Machine\Software\Classes\Interface\{AF86E2E0-B12D-4C6A-9C5A-D7AA65101E90}			
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{AF86E2E0-B12D-4c6a-9C5A-D7AA65101E90}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{AF86E2E0-B12D-4c6a-9C5A-D7AA65101E90}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\Interface\{AF86E2E0-B12D-4c6a-9C5A-D7AA65101E90}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{AF86E2E0-B12D-4c6a-9C5A-D7AA65101E90}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x00000444 ObjectAttributesHandle: 0x0000041a ObjectAttributesName: ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x00000446 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{AF86E2E0-B12D-4c6a-9C5A-D7AA65101E90}\ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x00000446 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{AF86E2E0-B12D-4c6a-9C5A-D7AA65101E90}\ProxyStubClsid32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500 Classes\WOW6432Node\Interface\{AF86E2E0-B12D-4c6a-9C5A-D7AA65101E90}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: {00000320-0000-0000-C000-000000000046} KeyHandle: 0x00000446 ValueName: Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{AF86E2E0-B12D-4c6a-9C5A-D7AA65101E90}\ProxyStubClsid32\(Default)	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x00000446	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x0000041a	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x00000418	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x00000444	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQuerySystemTime**		success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000002c6 KeyInformation: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000002c6 KeyInformation: \x01\x00\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Interface\{89BC3F49-F8D9-5103-BA13-DE497E609167} DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000002c6 ObjectAttributesName: Interface\{89BC3F49-F8D9-5103-BA13-DE497E609167}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\Software\Classes\Interface\{89BC3F49-F8D9-5103-BA13-DE497E609167} DesiredAccess: KEY_READ KeyHandle: 0x00000418 ObjectAttributesHandle: 0x00000000	success	0x00000000	

				ObjectAttributesName: \Registry\Machine\Software\Classes\Interface\{89BC3F49-F8D9-5103-BA13-DE497E609167}			
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000041a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{89bc3f49-f8d9-5103-ba13-de497e609167}	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000041a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{89bc3f49-f8d9-5103-ba13-de497e609167}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\Interface\{89bc3f49-f8d9-5103-ba13-de497e609167}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{89bc3f49-f8d9-5103-ba13-de497e609167}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x00000448 ObjectAttributesHandle: 0x0000041a ObjectAttributesName: ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x0000044a KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{89bc3f49-f8d9-5103-ba13-de497e609167}\ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x0000044a KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{89bc3f49-f8d9-5103-ba13-de497e609167}\ProxyStubClsid32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\Interface\{89bc3f49-f8d9-5103-ba13-de497e609167}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtQueryValueKey**	Information: {c53e07ec-25f3-4093-aa39-fc67ea22e99d} KeyHandle: 0x0000044a ValueName: Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{89bc3f49-f8d9-5103-ba13-de497e609167}\ProxyStubClsid32\(Default)	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x0000044a	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x0000041a	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,815	7476	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,815	5280	0x00632d59 0x0040122a	**CoCreateInstance**	rclsid: 0340F119-A598-4ED9-B0AC-6F6A12D3E755 ProgID: ClsContext: CLSCTX_INPROC_SERVER riid: 7F73BE3F-FB79-493C-A6C7-7EE14E245841	success	0x00000000	
2019-04-18 21:18:24,815	5280	0x00632d59 0x0040122a	**CoCreateInstance**	rclsid: 76765B11-3F95-4AF2-AC9D-EA55D8994F1A ProgID: ClsContext: CLSCTX_INPROC_SERVER riid: 00000000-0000-0000-C000-000000000046	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x00000418 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x00000418	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000	**NtProtectVirtualMemory**	StackPivoted: no	success	0x00000000	

		0x00000000		OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000			
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtOpenKey**	ObjectAttributes:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.Application DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED KeyHandle: 0x000004a0 ObjectAttributesHandle: 0x0000042c ObjectAttributesName: Windows.Internal.StateRepository.Application	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 0 KeyHandle: 0x000004a0 KeyInformation:\xef\xbe\xb8\xef\xbe\xa3^\xef\xbe\x9e\xef\xbf\x9b3\xef\xbf\x94\x01\x00\x00\x00\x00X\x00\x00\x00W\x00i\x00n\x00d\x00o\x00w\x00s\x00.\x00I\x00n\x00t\x00e\x00r\x00n\x00a\x00l\x00.\x00S\x00t\x00a\x00t\x00e\x00R\x00e\x00p\x00o\x00s\x00i\x00t\x00o\x00r\x00y\x00.\x00A\x00p\x00p\x00l\x00i\x00c\x00a\x00t\x00i\x00o\x00n\x00\x10\x00\x00\x00(\x00\x00\x00\x05\x00\x00\x00\x00\x00\x00\x00\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x08\xef\xbe\xbdf\x008\xef\xbe\x99\xef\xbf\x93\x02T\xef\xbf\xb5\xef\xbf\xad\x04\xef\xbf\xaeGuwX\xef\xbf\xa6b\x00\xef\xbf\xaeGuw\x00\x00\x00\x00\x00\x00\x00\x008\xef\xbe\xbce\x008\xef\xbe\xbce\x00\xef\xbf\x80\x00^\x00\xef\xbf\x88\xef\xbf\xb6\xef\xbf\xad\x04\xef\xbe\x8dc\xef\xbf\xa8t\x02\x00\x00\x00\xef\xbf\xaac\xef\xbf\xa8t\xef\xbf\xa0\xef\xbf\x83\x00u0U\xef\xbf\xa8t(\xef\xbe\xb7d\x00\xef\xbf\x8ed\xef\xbf\xa8t\xef\xbe\x90\x00\x00\x00(\xef\xbe\xb7d\x00\x01\x00\x00\x00\x04\x00\x00\x00\x08\xef\xbe\xbdf\x00\xef\xbf\xa0\xef\xbf\x83\x00u\x01\x00\x00\x00\x00\x00\x00\xef\xbf\x88\x18\x13{ \x00\x04\x008\xef\xbe\xbce\x00<\xef\xbe\xb7d\x00\x00\x00^\x00X\xef\xbf\xb6\xef\xbf\xad\x04\x01\x00\x00\x00 \xef\xbe\xa3\x00u\xef\xbf\xb0\xef\xbf\x9fd\x00\xef\xbe\x83\x00\x00\x000U\xef\xbf\xa8t8\x00\x00\x00\x00\x00^\x00x\ \xef\xbf\xb6\xef\xbf\xad\x04\x00\x00\x00\x00D\x00\x00\x00\x00\x00^\x00\xef\xbe\x88\xef\xbf\xb6\xef\xbf\xad\x04\x00 \x00\x02\x00@\x00\x00\x00\xef\xbf\x90\x07\x02\x00\x00\x00\x02\x00\x00\x00\x00\x00P\x00\x00\x00\xef\xbf\x90\x07\x02\x00\xef\xbf\x9e\xef\xbf\x81\x00\x00\x00\x00\x00\x00x\xef\xbe\x9eb\x00\xef\xbf\x88\xef\xbe\xafd\x00\xef\xbf\x9f\xef\xbf\x81\x02\x00\x00\x00\x02\x00\x06\x00\x00\x00\x13$0\x06\x00\x00\x02\x00\xef\xbf\xa8\xef\xbe\xafd\x00\x17\x00\x00\x00\x08\xef\xbe\xbdf\x00 \x00\x00\x00H\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x10\x0c\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x008\xef\xbe\xbce\x00D\x00\x00\x00\x00\x00\x00\x00X\xef\xbf\xa6b\x00\x00\x00^\x00\x02\x00\x00\x00P\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x02\x00\x00\x00\x00\x00\x00\x00\x00D\x00\x00\x00\x00\x00\x00\x00\x00(\xef\xbe\xb7d\x00\xef\xbf\xaeGuw\xef\xbe\xa4\xef\xbf\xb6\xef\xbf\xad\x04\xef\xbf\xaeGuw\x00\x00\x00\x00\xef\xbf\xaeGuw\x00\x00\x00\x00\x00\x00\x00\x00\x008\xef\xbe\xbce\x00X\xef\xbf\xa6b\x00p\xef\xbf\xa6b\x00(\xef\xbe\xb7d\x008\xef\xbe\xbce\x00\xef\xbf\x90\xef\xbf\xb6\xef\xbf\xad\x04	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	Information: 1 KeyHandle: 0x000004a0 ValueName: ActivationType Type: REG_DWORD FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.Application\ActivationType	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	Information: StateRepository KeyHandle: 0x000004a0	success	0x00000000	

				ValueName: Server Type: REG_SZ FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.Application\Server			
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.Application\DllPath KeyHandle: 0x000004a0 ValueName: DllPath	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.Application\Threading KeyHandle: 0x000004a0 ValueName: Threading	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	Information: 0 KeyHandle: 0x000004a0 ValueName: TrustLevel Type: REG_DWORD FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.Application\TrustLevel	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.Application\CustomAttributes DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000004a0 ObjectAttributesName: CustomAttributes	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.Application\RemoteServer KeyHandle: 0x000004a0 ValueName: RemoteServer	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.Application\ActivateAsUser KeyHandle: 0x000004a0 ValueName: ActivateAsUser	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.Application\ActivateInSharedBroker KeyHandle: 0x000004a0 ValueName: ActivateInSharedBroker	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.Application\Permissions KeyHandle: 0x000004a0 ValueName: Permissions	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x000004a0	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtDuplicateObject**	TargetHandle: 0x000004a4 TargetProcessHandle: 0xffffffff Options: DUPLICATE_SAME_ACCESS SourceHandle: 0xfffffffe SourceProcessHandle: 0xffffffff	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtDuplicateObject**	TargetHandle: 0x000004ac TargetProcessHandle: 0xffffffff Options: DUPLICATE_SAME_ACCESS SourceHandle: 0xfffffffe SourceProcessHandle: 0xffffffff	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**CoCreateInstance**	rclsid: 00000339-0000-0000-C000-000000000046 ProgID: ClsContext: CLSCTX_NO_CODE_DOWNLOAD|CLSCTX_INPROC_HANDLER|CLSCTX_INPROC_SERVER riid: 00000003-0000-0000-C000-000000000046	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000002c6 KeyInformation: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000002c6 KeyInformation: \x01\x00\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Interface\{D81E96F1-A89C-417E-9335-59531026309D} DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000002c6 ObjectAttributesName: Interface\{D81E96F1-A89C-417E-9335-59531026309D}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\Software\Classes\Interface\{D81E96F1-A89C-417E-9335-59531026309D} DesiredAccess: KEY_READ	success	0x00000000	

				KeyHandle: 0x000004b0 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \Registry\Machine\Software\Classes\Interface\{D81E96F1-A89C-417E-9335-59531026309D}			
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000004b2 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{d81e96f1-a89c-417e-9335-59531026309d}	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000004b2 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{d81e96f1-a89c-417e-9335-59531026309d}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500 Classes\WOW6432Node\Interface\{d81e96f1-a89c-417e-9335-59531026309d}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{d81e96f1-a89c-417e-9335-59531026309d}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x000004b4 ObjectAttributesHandle: 0x000004b2 ObjectAttributesName: ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000004b6 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{d81e96f1-a89c-417e-9335-59531026309d}\ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000004b6 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{d81e96f1-a89c-417e-9335-59531026309d}\ProxyStubClsid32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500 Classes\WOW6432Node\Interface\{d81e96f1-a89c-417e-9335-59531026309d}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	Information: {c53e07ec-25f3-4093-aa39-fc67ea22e99d} KeyHandle: 0x000004b6 ValueName: Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{d81e96f1-a89c-417e-9335-59531026309d}\ProxyStubClsid32\(Default)	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x000004b6	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x000004b2	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtOpenKey**	ObjectAttributes:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.ApplicationExtension DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED KeyHandle: 0x000004b0 ObjectAttributesHandle: 0x0000042c ObjectAttributesName: Windows.Internal.StateRepository.ApplicationExtension	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 0 KeyHandle: 0x000004b0	success	0x00000000	

				KeyInformation:\xef\xbe\xb8\xef\xbe\xa3^\xef\xbe\x9e\xef\xbf\x9b3\xef\xbf\x94\x01\x00\x00\x00\x00j\x00\x00\x00W\x00i\x00n\x00d\x00o\x00w\x00s\x00.\x00I\x00n\x00t\x00e\x00r\x00n\x00a\x00l\x00.\x00S\x00t\x00a\x00t\x00e\x00R\x00e\x00p\x00o\x00s\x00i\x00t\x00o\x00r\x00y\x00.\x00A\x00p\x00p\x00l\x00i\x00c\x00a\x00t\x00i\x00o\x00n\x00E\x00x\x00t\x00e\x00n\x00s\x00i\x00o\x00n\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xef\xbf\x80\xef\xbe\xbef\x00\x00\x00^\x00T\xef\xbf\xb5\xef\xbf\xad\x04\xef\xbf\xaeGuw\xef\xbf\x98\xef\xbf\xa7b\x00\xef\xbf\xaeGuw\x00\x00\x00\x00\x00\x00\x00\x00\xef\xbf\xa8\xef\xbf\x8bb\x00\xef\xbf\xa8\xef\xbf\x8bb\x00\xef\xbf\x80\x00^\x00\xef\xbf\x88\xef\xbf\xb6\xef\xbf\xad\x04\xef\xbe\x8dc\xef\xbf\xa8t\x02\x00\x00\x00\xef\xbf\xaac\xef\xbf\xa8t\xef\xbf\xa0\xef\xbf\x83\x00u0U\xef\xbf\xa8tx\xef\xbe\xb2d\x00\xef\xbf\x8ed\xef\xbf\xa8t\xef\xbe\x90\x00\x00\x00\x00x\xef\xbe\xb2d\x00\x01\x00\x00\x00\xef\xbf\xb0\x00\x00\x00\xef\xbf\x80\xef\xbe\xbef\x00\xef\xbf\xa0\xef\xbf\x83\x00u\x01\x00\x00\x00\x00\x00\x00\x00\x04E\xef\xbf\x9ft\x00\x00p\x01\xef\xbf\xa8\xef\xbf\x8bb\x00\xef\xbe\x8c\xef\xbe\xb2d\x00\x00\x00^\x00X\xef\xbf\xb6\xef\xbf\xad\x04\x01\x00\x00\x00\xef\xbe\xa3\x00u\xef\xbf\xb0\xef\xbf\x9fd\x00\xef\xbf\x80\x00^\x000U\xef\xbf\xa8t8\x00\x00\x00\x00\x00^\x00x\xef\xbf\xb6\xef\xbf\xad\x04\x00\x00\x00\x00D\x00\x00\x00\x00\x00^\x00\xef\xbe\x88\xef\xbf\xb6\xef\xbf\xad\x04\x00\x00\x02\x00@\x00\x00\x00\xef\xbf\x90\x07\x02\x00\x00\x00\x02\x00\x00\x00\x00P\x00\x00\x00\xef\xbf\x90\x07\x02\x00\xef\xbf\xafl\x00\x00\x00\x00\x00\x00x\xef\xbe\x9eb\x00\xef\xbf\x88\xef\xbe\xafd\x00\xef\xbf\xb01\x02\x00\x00\x00\x02\x00\x0c\x00\x00\x003$0\x06\x00\x00\x02\x00\xef\xbf\xa4\xef\xbe\xafd\x00\x08\x00\x00\x00\xef\xbf\x80\xef\xbe\xbef\x00 \x00\x00\x00H\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x10\x0c\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\xef\xbf\xa8\xef\xbf\x8bb\x00D\x00\x00\x00\x00\x00\x00\x00\xef\xbf\x98\xef\xbf\xa7b\x00\x00\x00^\x00\x02\x00\x00\x00P\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x02\x00\x00\x00\x00\x00\x00\x00D\x00\x00\x00\x00\x00\x00\x00x\xef\xbe\xb2d\x00\xef\xbf\xaeGuw\xef\xbe\xa4\xef\xbf\xb6\xef\xbf\xad\x04\xef\xbf\xaeGuw\x00\x00\x00\x00\xef\xbf\xaeGuw\x00\x00\x00\x00\x00\x00\x00\x00\xef\xbf\xa8\xef\xbf\x8bb\x00\xef\xbf\x98\xef\xbf\xa7b\x00\xef\xbf\xb0\xef\xbf\xa7b\x00x\xef\xbe\xb2d\x00\xef\xbf\xa8\xef\xbf\x8bb\x00\xef\xbf\x90\xef\xbf\xb6\xef\xbf\xad\x04			
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	Information: 1 KeyHandle: 0x000004b0 ValueName: ActivationType Type: REG_DWORD FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.ApplicationExtension\ActivationType	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	Information: StateRepository KeyHandle: 0x000004b0 ValueName: Server Type: REG_SZ FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.ApplicationExtension\Server	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.ApplicationExtension\DllPath KeyHandle: 0x000004b0 ValueName: DllPath	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.ApplicationExtension\Threading KeyHandle: 0x000004b0 ValueName: Threading	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	Information: 0 KeyHandle: 0x000004b0 ValueName: TrustLevel Type: REG_DWORD FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.ApplicationExtension\TrustLevel	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.ApplicationExtension\CustomAttributes DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000004b0 ObjectAttributesName: CustomAttributes	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.ApplicationExtension\RemoteServer KeyHandle: 0x000004b0 ValueName: RemoteServer	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.ApplicationExtension\ActivateAsUser KeyHandle: 0x000004b0 ValueName: ActivateAsUser	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.ApplicationExtension\ActivateInSharedBroker KeyHandle: 0x000004b0 ValueName: ActivateInSharedBroker	failed	OBJECT_NAME_NOT_FOUND	

2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	FullName:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Internal.StateRepository.ApplicationExtension\Permissions KeyHandle: 0x000004b0 ValueName: Permissions	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x000004b0	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**CoCreateInstance**	rclsid: 00000339-0000-0000-C000-000000000046 ProgID: ClsContext: CLSCTX_NO_CODE_DOWNLOAD|CLSCTX_INPROC_HANDLER|CLSCTX_INPROC_SERVER riid: 00000003-0000-0000-C000-000000000046	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000002c6 KeyInformation: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000002c6 KeyInformation: \x01\x00\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Interface\{78662BBB-1464-4279-B5FF-FFCCB2BC6529} DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000002c6 ObjectAttributesName: Interface\{78662BBB-1464-4279-B5FF-FFCCB2BC6529}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\Software\Classes\Interface\{78662BBB-1464-4279-B5FF-FFCCB2BC6529} DesiredAccess: KEY_READ KeyHandle: 0x000004b0 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \Registry\Machine\Software\Classes\Interface\{78662BBB-1464-4279-B5FF-FFCCB2BC6529}	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000004b2 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{78662bbb-1464-4279-b5ff-ffccb2bc6529}	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000004b2 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{78662bbb-1464-4279-b5ff-ffccb2bc6529}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\Interface\{78662bbb-1464-4279-b5ff-ffccb2bc6529}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{78662bbb-1464-4279-b5ff-ffccb2bc6529}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x000004b4 ObjectAttributesHandle: 0x000004b2 ObjectAttributesName: ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000004b6 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{78662bbb-1464-4279-b5ff-ffccb2bc6529}\ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000004b6 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{78662bbb-1464-4279-b5ff-ffccb2bc6529}\ProxyStubClsid32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\Interface\{78662bbb-1464-4279-b5ff-ffccb2bc6529}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtQueryValueKey**	Information: {c53e07ec-25f3-4093-aa39-fc67ea22e99d} KeyHandle: 0x000004b6 ValueName: Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{78662bbb-1464-4279-b5ff-ffccb2bc6529}\ProxyStubClsid32\(Default)	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x000004b6	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000	**NtClose**	Handle: 0x000004b2	success	0x00000000	

		0x00000000					
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,815	1044	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000002c6 KeyInformation: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000002c6 KeyInformation: \x01\x00\x00\x00	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Interface\{DD692782-932C-53A0-90CA-70249EBFA3D9} DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000002c6 ObjectAttributesName: Interface\{DD692782-932C-53A0-90CA-70249EBFA3D9}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\Software\Classes\Interface\{DD692782-932C-53A0-90CA-70249EBFA3D9} DesiredAccess: KEY_READ KeyHandle: 0x000004b0 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \Registry\Machine\Software\Classes\Interface\{DD692782-932C-53A0-90CA-70249EBFA3D9}	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000004b2 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{dd692782-932c-53a0-90ca-70249ebfa3d9}	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000004b2 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{dd692782-932c-53a0-90ca-70249ebfa3d9}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\Interface\{dd692782-932c-53a0-90ca-70249ebfa3d9}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{dd692782-932c-53a0-90ca-70249ebfa3d9}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x000004b4 ObjectAttributesHandle: 0x000004b2 ObjectAttributesName: ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000004b6 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{dd692782-932c-53a0-90ca-70249ebfa3d9}\ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000004b6 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{dd692782-932c-53a0-90ca-70249ebfa3d9}\ProxyStubClsid32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\Interface\{dd692782-932c-53a0-90ca-70249ebfa3d9}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryValueKey**	Information: {c53e07ec-25f3-4093-aa39-fc67ea22e99d} KeyHandle: 0x000004b6 ValueName: Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{dd692782-932c-53a0-90ca-70249ebfa3d9}\ProxyStubClsid32\(Default)	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x000004b6	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000	**NtClose**	Handle: 0x000004b2	success	0x00000000	

		0x00000000					
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000002c6 KeyInformation: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000002c6 KeyInformation: \x01\x00\x00\x00	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Interface\{5B086F31-E193-4811-A185-6DB2816D1691} DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000002c6 ObjectAttributesName: Interface\{5B086F31-E193-4811-A185-6DB2816D1691}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\Software\Classes\Interface\{5B086F31-E193-4811-A185-6DB2816D1691} DesiredAccess: KEY_READ KeyHandle: 0x000004b0 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \Registry\Machine\Software\Classes\Interface\{5B086F31-E193-4811-A185-6DB2816D1691}	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000004b2 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{5b086f31-e193-4811-a185-6db2816d1691}	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000004b2 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{5b086f31-e193-4811-a185-6db2816d1691}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500 Classes\WOW6432Node\Interface\{5b086f31-e193-4811-a185-6db2816d1691}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{5b086f31-e193-4811-a185-6db2816d1691}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x000004b4 ObjectAttributesHandle: 0x000004b2 ObjectAttributesName: ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000004b6 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{5b086f31-e193-4811-a185-6db2816d1691}\ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000004b6 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{5b086f31-e193-4811-a185-6db2816d1691}\ProxyStubClsid32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500 Classes\WOW6432Node\Interface\{5b086f31-e193-4811-a185-6db2816d1691}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryValueKey**	Information: {c53e07ec-25f3-4093-aa39-fc67ea22e99d} KeyHandle: 0x000004b6 ValueName: Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{5b086f31-e193-4811-a185-6db2816d1691}\ProxyStubClsid32\(Default)	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x000004b6	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000	**NtClose**	Handle: 0x000004b2	success	0x00000000	

		0x00000000					
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000002c6 KeyInformation: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000002c6 KeyInformation: \x01\x00\x00\x00	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Interface\{7BF24DE6-6FFA-585B-92FC-EF9D24FB1023} DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x000002c6 ObjectAttributesName: Interface\{7BF24DE6-6FFA-585B-92FC-EF9D24FB1023}	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\Software\Classes\Interface\{7BF24DE6-6FFA-585B-92FC-EF9D24FB1023} DesiredAccess: KEY_READ KeyHandle: 0x000004b0 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \Registry\Machine\Software\Classes\Interface\{7BF24DE6-6FFA-585B-92FC-EF9D24FB1023}	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000004b2 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{7bf24de6-6ffa-585b-92fc-ef9d24fb1023}	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000004b2 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{7bf24de6-6ffa-585b-92fc-ef9d24fb1023}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\Interface\{7bf24de6-6ffa-585b-92fc-ef9d24fb1023}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{7bf24de6-6ffa-585b-92fc-ef9d24fb1023}\ProxyStubClsid32 DesiredAccess: KEY_READ KeyHandle: 0x000004b4 ObjectAttributesHandle: 0x000004b2 ObjectAttributesName: ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 3 KeyHandle: 0x000004b6 KeyInformation: \REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{7bf24de6-6ffa-585b-92fc-ef9d24fb1023}\ProxyStubClsid32	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryKey**	KeyInformationClass: 7 KeyHandle: 0x000004b6 KeyInformation: \x01\x04\x00\x00	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\WOW6432Node\Interface\{7bf24de6-6ffa-585b-92fc-ef9d24fb1023}\ProxyStubClsid32 DesiredAccess: MAXIMUM_ALLOWED KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500_Classes\WOW6432Node\Interface\{7bf24de6-6ffa-585b-92fc-ef9d24fb1023}\ProxyStubClsid32	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtQueryValueKey**	Information: {c53e07ec-25f3-4093-aa39-fc67ea22e99d} KeyHandle: 0x000004b6 ValueName: Type: REG_SZ FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\Interface\{7bf24de6-6ffa-585b-92fc-ef9d24fb1023}\ProxyStubClsid32\(Default)	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x000004b6	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000	**NtClose**	Handle: 0x000004b2	success	0x00000000	

		0x00000000					
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002c0 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:24,831	1044	0x00000000 0x00000000	**CoCreateInstance**	rclsid: 00000352-0000-0000-C000-000000000046 ProgID: ClsContext: CLSCTX_NO_CODE_DOWNLOAD|CLSCTX_INPROC_HANDLER|CLSCTX_INPROC_SERVER riid: 00000003-0000-0000-C000-000000000046	success	0x00000000	88 times
2019-04-18 21:18:24,878	1044	0x00000000 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:24,878	1044	0x00000000 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74775000	success	0x00000000	
2019-04-18 21:18:24,878	5280	0x00632d59 0x0040122a	**CoCreateInstance**	rclsid: F324E4F9-8496-40B2-A1FF-9617C1C9AFFE ProgID: ClsContext: CLSCTX_INPROC_SERVER riid: 387FDB83-DD33-4995-9D2D-1F647E846705	success	0x00000000	
2019-04-18 21:18:24,878	5280	0x00632d59 0x0040122a	**CoCreateInstance**	rclsid: 0340F119-A598-4ED9-B0AC-6F6A12D3E755 ProgID: ClsContext: CLSCTX_INPROC_SERVER riid: 7F73BE3F-FB79-493C-A6C7-7EE14E245841	success	0x00000000	
2019-04-18 21:18:24,878	5280	0x00632d59 0x0040122a	**CoCreateInstance**	rclsid: 7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4 ProgID: ClsContext: CLSCTX_INPROC_SERVER riid: 79EAC9EE-BAF9-11CE-8C82-00AA004BA90B	success	0x00000000	
2019-04-18 21:18:24,878	5280	0x00632d59 0x0040122a	**CoCreateInstance**	rclsid: 0340F119-A598-4ED9-B0AC-6F6A12D3E755 ProgID: ClsContext: CLSCTX_INPROC_SERVER riid: 7F73BE3F-FB79-493C-A6C7-7EE14E245841	success	0x00000000	
2019-04-18 21:18:24,878	5280	0x00632d59 0x0040122a	**CoCreateInstance**	rclsid: CDC82860-468D-4D4E-B7E7-C298FF23AB2C ProgID: ClsContext: CLSCTX_INPROC_SERVER riid: 5632B1A4-E38A-400A-928A-D4CD63230295	success	0x00000000	
2019-04-18 21:18:24,878	5280	0x00632d59 0x0040122a	**CoCreateInstance**	rclsid: 0340F119-A598-4ED9-B0AC-6F6A12D3E755 ProgID: ClsContext: CLSCTX_INPROC_SERVER riid: 7F73BE3F-FB79-493C-A6C7-7EE14E245841	success	0x00000000	2 times
2019-04-18 21:18:24,893	5280	0x00632d59 0x0040122a	**ShellExecuteExW**	Show: SW_SHOWNORMAL Parameters: FilePath: C:\Users\Administrator\suoes.exe	success	0x00000001	
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,893	5280	0x00632d45 0x0040122a	**CreateToolhelp32Snapshot**	Flags: TH32CS_SNAPPROCESS ProcessId: 0	success	0x000003a0	
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,893	5280	0x00632d45 0x0040122a	**Process32FirstW**	ProcessName: [System Process] ProcessId: 0	success	0x00000001	
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,893	5280	0x00632d45	**Process32NextW**	ProcessName: System	success	0x00000001	

		0x0040122a		ProcessId: 4			
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	1 time
2019-04-18 21:18:24,893	5280	0x00632d4a 0x0040122a	**NtOpenProcess**	ProcessHandle: 0x00000000 ProcessIdentifier: 4 DesiredAccess: PROCESS_ALL_ACCESS	failed	ACCESS_DENIED	
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,893	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x00000000	failed	INVALID_HANDLE	
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,893	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: Registry ProcessId: 88	success	0x00000001	
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,893	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: smss.exe ProcessId: 328	success	0x00000001	
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,893	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: csrss.exe ProcessId: 424	success	0x00000001	
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,893	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: wininit.exe ProcessId: 496	success	0x00000001	
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,893	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: csrss.exe ProcessId: 504	success	0x00000001	
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,893	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: winlogon.exe ProcessId: 588	success	0x00000001	
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,893	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: services.exe ProcessId: 624	success	0x00000001	
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,893	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: lsass.exe ProcessId: 632	success	0x00000001	
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,893	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 736	success	0x00000001	
2019-04-18 21:18:24,893	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,909	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: fontdrvhost.exe ProcessId: 744	success	0x00000001	
2019-04-18 21:18:24,909	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,909	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: fontdrvhost.exe ProcessId: 752	success	0x00000001	
2019-04-18 21:18:24,909	5280	0x0040122a	**LdrLoadDll**	Flags: 0x00000000	success	0x00000000	

		0x00000000		BaseAddress: 0x00000000 FileName: kernel32			
2019-04-18 21:18:24,909	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 820	success	0x00000001	
2019-04-18 21:18:24,909	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,909	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 872	success	0x00000001	
2019-04-18 21:18:24,909	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,909	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 916	success	0x00000001	
2019-04-18 21:18:24,909	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,909	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: dwm.exe ProcessId: 1000	success	0x00000001	
2019-04-18 21:18:24,909	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,909	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 384	success	0x00000001	
2019-04-18 21:18:24,909	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,909	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 416	success	0x00000001	
2019-04-18 21:18:24,909	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,909	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 404	success	0x00000001	
2019-04-18 21:18:24,909	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,909	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 560	success	0x00000001	
2019-04-18 21:18:24,909	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,909	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1072	success	0x00000001	
2019-04-18 21:18:24,909	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1084	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1132	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1140	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1240	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45	**Process32NextW**	ProcessName: svchost.exe	success	0x00000001	

		0x0040122a		ProcessId: 1252			
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1308	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1340	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1436	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1516	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1524	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1540	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: Memory Compression ProcessId: 1600	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1660	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1684	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1708	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1716	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1796	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1856	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000	success	0x00000000	

				FileName: kernel32			
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1868	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1884	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2000	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 964	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1848	success	0x00000001	
2019-04-18 21:18:24,925	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,925	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2088	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: spoolsv.exe ProcessId: 2216	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2272	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2292	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2424	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2444	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2452	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2460	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: WmiPrvSE.exe ProcessId: 2584	success	0x00000001	

2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: OfficeClickToRun.exe ProcessId: 2644	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: Sysmon64.exe ProcessId: 2684	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2708	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2720	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2740	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: SecurityHealthService.exe ProcessId: 2748	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2780	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2804	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2820	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2908	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 3152	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 3244	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: unsecapp.exe ProcessId: 3256	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	

2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 3604	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 3692	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 3936	success	0x00000001	
2019-04-18 21:18:24,940	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,940	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: WmiPrvSE.exe ProcessId: 3992	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 3024	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 3912	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 3268	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: sedsvc.exe ProcessId: 1676	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: SgrmBroker.exe ProcessId: 1472	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 2796	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: SearchIndexer.exe ProcessId: 1644	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 884	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: SearchProtocolHost.exe ProcessId: 1696	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: SearchFilterHost.exe ProcessId: 1272	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a	**LdrLoadDll**	Flags: 0x00000000	success	0x00000000	

		0x00000000		BaseAddress: 0x00000000 FileName: kernel32			
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: sihost.exe ProcessId: 1180	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 3252	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 3884	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: taskhostw.exe ProcessId: 4232	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	1 time
2019-04-18 21:18:24,956	5280	0x00632d4a 0x0040122a	**NtOpenProcess**	ProcessHandle: 0x000004b0 ProcessIdentifier: 4232 DesiredAccess: PROCESS_ALL_ACCESS	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d40 0x0040122a	**LdrGetDllHandle**	ModuleHandle: 0x76740000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	2 times
2019-04-18 21:18:24,956	5280	0x00632d54 0x0040122a	**WriteProcessMemory**	Buffer: StackPivoted: no ProcessHandle: 0x000004b0 BufferLength: 0x00000000 BaseAddress: 0x76756510	failed	0x00000000	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d54 0x0040122a	**WriteProcessMemory**	Buffer: StackPivoted: no ProcessHandle: 0x000004b0 BufferLength: 0x00000000 BaseAddress: 0x76756530	failed	0x00000000	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x76756510	failed	INVALID_HANDLE	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x76756530	failed	INVALID_HANDLE	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x000004b0	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,956	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 4256	success	0x00000001	
2019-04-18 21:18:24,956	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000	success	0x00000000	

				FileName: kernel32			
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 4352	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 4404	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: ctfmon.exe ProcessId: 4420	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: explorer.exe ProcessId: 4596	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 4680	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 4764	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: ShellExperienceHost.exe ProcessId: 4384	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 4288	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 4208	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: SearchUI.exe ProcessId: 5128	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: RuntimeBroker.exe ProcessId: 5248	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: smartscreen.exe ProcessId: 5412	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: RuntimeBroker.exe ProcessId: 5496	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: ApplicationFrameHost.exe ProcessId: 5608	success	0x00000001	

2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: SearchProtocolHost.exe ProcessId: 6676	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: backgroundTaskHost.exe ProcessId: 7032	success	0x00000001	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	1 time
2019-04-18 21:18:24,971	5280	0x00632d4a 0x0040122a	**NtOpenProcess**	ProcessHandle: 0x000004b0 ProcessIdentifier: 7032 DesiredAccess: PROCESS_ALL_ACCESS	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d40 0x0040122a	**LdrGetDllHandle**	ModuleHandle: 0x76740000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	2 times
2019-04-18 21:18:24,971	5280	0x00632d54 0x0040122a	**WriteProcessMemory**	Buffer: StackPivoted: no ProcessHandle: 0x000004b0 BufferLength: 0x00000000 BaseAddress: 0x76756510	failed	0x00000000	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d54 0x0040122a	**WriteProcessMemory**	Buffer: StackPivoted: no ProcessHandle: 0x000004b0 BufferLength: 0x00000000 BaseAddress: 0x76756530	failed	0x00000000	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x76756510	failed	INVALID_HANDLE	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,971	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x76756530	failed	INVALID_HANDLE	
2019-04-18 21:18:24,971	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x000004b0	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: RuntimeBroker.exe ProcessId: 6872	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: FileCoAuth.exe ProcessId: 6980	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 5764	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a	**LdrLoadDll**	Flags: 0x00000000	success	0x00000000	

		0x00000000		BaseAddress: 0x00000000 FileName: kernel32			
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: OneDrive.exe ProcessId: 5820	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 5860	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: jusched.exe ProcessId: 6280	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: dllhost.exe ProcessId: 4092	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: BackgroundTransferHost.exe ProcessId: 6928	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: rundll32.exe ProcessId: 1372	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: RuntimeBroker.exe ProcessId: 5896	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: RuntimeBroker.exe ProcessId: 4980	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 4464	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 6752	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 7180	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 7480	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: backgroundTaskHost.exe ProcessId: 7748	success	0x00000001	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	1 time
2019-04-18 21:18:24,987	5280	0x00632d4a	**NtOpenProcess**	ProcessHandle: 0x000004b0	success	0x00000000	

		0x0040122a		ProcessIdentifier: 7748 DesiredAccess: PROCESS_ALL_ACCESS			
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d40 0x0040122a	**LdrGetDllHandle**	ModuleHandle: 0x76740000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	2 times
2019-04-18 21:18:24,987	5280	0x00632d54 0x0040122a	**WriteProcessMemory**	Buffer: StackPivoted: no ProcessHandle: 0x000004b0 BufferLength: 0x00000000 BaseAddress: 0x76756510	failed	0x00000000	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d54 0x0040122a	**WriteProcessMemory**	Buffer: StackPivoted: no ProcessHandle: 0x000004b0 BufferLength: 0x00000000 BaseAddress: 0x76756530	failed	0x00000000	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x76756510	failed	INVALID_HANDLE	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:24,987	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x76756530	failed	INVALID_HANDLE	
2019-04-18 21:18:24,987	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x000004b0	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: RuntimeBroker.exe ProcessId: 7848	success	0x00000001	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: backgroundTaskHost.exe ProcessId: 7904	success	0x00000001	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	1 time
2019-04-18 21:18:25,003	5280	0x00632d4a 0x0040122a	**NtOpenProcess**	ProcessHandle: 0x000004b0 ProcessIdentifier: 7904 DesiredAccess: PROCESS_ALL_ACCESS	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d40 0x0040122a	**LdrGetDllHandle**	ModuleHandle: 0x76740000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	2 times
2019-04-18 21:18:25,003	5280	0x00632d54 0x0040122a	**WriteProcessMemory**	Buffer: StackPivoted: no ProcessHandle: 0x000004b0 BufferLength: 0x00000000 BaseAddress: 0x76756510	failed	0x00000000	
2019-04-18 21:18:25,003	5280	0x0040122a	**LdrLoadDll**	Flags: 0x00000000	success	0x00000000	

		0x00000000		BaseAddress: 0x00000000 FileName: kernel32			
2019-04-18 21:18:25,003	5280	0x00632d54 0x0040122a	**WriteProcessMemory**	Buffer: StackPivoted: no ProcessHandle: 0x000004b0 BufferLength: 0x00000000 BaseAddress: 0x76756530	failed	0x00000000	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x76756510	failed	INVALID_HANDLE	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x76756530	failed	INVALID_HANDLE	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x000004b0	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: RuntimeBroker.exe ProcessId: 7936	success	0x00000001	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: backgroundTaskHost.exe ProcessId: 8000	success	0x00000001	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	1 time
2019-04-18 21:18:25,003	5280	0x00632d4a 0x0040122a	**NtOpenProcess**	ProcessHandle: 0x000004b0 ProcessIdentifier: 8000 DesiredAccess: PROCESS_ALL_ACCESS	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d40 0x0040122a	**LdrGetDllHandle**	ModuleHandle: 0x76740000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	2 times
2019-04-18 21:18:25,003	5280	0x00632d54 0x0040122a	**WriteProcessMemory**	Buffer: StackPivoted: no ProcessHandle: 0x000004b0 BufferLength: 0x00000000 BaseAddress: 0x76756510	failed	0x00000000	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d54 0x0040122a	**WriteProcessMemory**	Buffer: StackPivoted: no ProcessHandle: 0x000004b0 BufferLength: 0x00000000 BaseAddress: 0x76756530	failed	0x00000000	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x76756510	failed	INVALID_HANDLE	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d40	**NtClose**	Handle: 0x76756530	failed	INVALID_HANDLE	

		0x0040122a					
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x000004b0	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: RuntimeBroker.exe ProcessId: 8060	success	0x00000001	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,003	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: sppsvc.exe ProcessId: 7244	success	0x00000001	
2019-04-18 21:18:25,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: OfficeC2RClient.exe ProcessId: 6568	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: taskhostw.exe ProcessId: 6636	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	1 time
2019-04-18 21:18:25,018	5280	0x00632d4a 0x0040122a	**NtOpenProcess**	ProcessHandle: 0x000004b0 ProcessIdentifier: 6636 DesiredAccess: PROCESS_ALL_ACCESS	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d40 0x0040122a	**LdrGetDllHandle**	ModuleHandle: 0x76740000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	2 times
2019-04-18 21:18:25,018	5280	0x00632d54 0x0040122a	**WriteProcessMemory**	Buffer: StackPivoted: no ProcessHandle: 0x000004b0 BufferLength: 0x00000000 BaseAddress: 0x76756510	failed	0x00000000	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d54 0x0040122a	**WriteProcessMemory**	Buffer: StackPivoted: no ProcessHandle: 0x000004b0 BufferLength: 0x00000000 BaseAddress: 0x76756530	failed	0x00000000	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x76756510	failed	INVALID_HANDLE	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x76756530	failed	INVALID_HANDLE	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x000004b0	success	0x00000000	

2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: wermgr.exe ProcessId: 4584	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: DeviceCensus.exe ProcessId: 6540	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: CompatTelRunner.exe ProcessId: 2884	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: OsfInstaller.exe ProcessId: 6560	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: OneDriveStandaloneUpdater.exe ProcessId: 7308	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 6212	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: TrustedInstaller.exe ProcessId: 6260	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: TiWorker.exe ProcessId: 5164	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: kiato.exe ProcessId: 5308	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: SppExtComObj.Exe ProcessId: 5848	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: AppHostRegistrationVerifier.exe ProcessId: 1348	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: conhost.exe ProcessId: 5800	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: conhost.exe ProcessId: 7624	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	

2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 1416	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 3716	success	0x00000001	
2019-04-18 21:18:25,018	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,018	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: svchost.exe ProcessId: 6256	success	0x00000001	
2019-04-18 21:18:25,034	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: CompatTelRunner.exe ProcessId: 7844	success	0x00000001	
2019-04-18 21:18:25,034	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x00632d45 0x0040122a	**Process32NextW**	ProcessName: suoes.exe ProcessId: 6088	success	0x00000001	
2019-04-18 21:18:25,034	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x00632d45 0x0040122a	**Process32NextW**		failed	0x00000000	
2019-04-18 21:18:25,034	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x00632d40 0x0040122a	**NtClose**	Handle: 0x000003a0	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: advapi32	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x00632d68 0x0040122a	**RegCreateKeyExW**	Handle: 0x000003a0 FullName: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\ Access:KEY_QUERY_VALUE|KEY_SET_VALUE|KEY_CREATE_SUB_KEY|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_CREATE_LINK Registry: HKEY_CURRENT_USER Disposition: REG_OPENED_EXISTING_KEY Class: SubKey: Software\Microsoft\Windows\CurrentVersion\Run\	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: advapi32	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0068d7c1 0x0040122a	**RegSetValueExW**	Handle: 0x000003a0 Buffer: C:\Users\Administrator\suoes.exe /n BufferLength: 70 ValueName: suoes Type: REG_SZ FullName: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\suoes	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: advapi32	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0068d7a8 0x0040122a	**RegCloseKey**	Handle: 0x000003a0	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: advapi32	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0068d7d0 0x0040122a	**RegCreateKeyExW**	Handle: 0x000003a0 FullName: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ Access:KEY_QUERY_VALUE|KEY_SET_VALUE|KEY_CREATE_SUB_KEY|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_CREATE_LINK Registry: HKEY_CURRENT_USER Disposition: REG_OPENED_EXISTING_KEY Class: SubKey: Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\	success	0x00000000	

2019-04-18 21:18:25,034	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: advapi32	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0068d7c1 0x0040122a	**RegSetValueExW**	Handle: 0x000003a0 Buffer: 0 BufferLength: 4 ValueName: ShowSuperHidden Type: REG_DWORD FullName:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: advapi32	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0068d7a8 0x0040122a	**RegCloseKey**	Handle: 0x000003a0	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: advapi32	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0068d7d0 0x0040122a	**RegCreateKeyExW**	Handle: 0x000004b4 FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU Access:KEY_QUERY_VALUE|KEY_SET_VALUE|KEY_CREATE_SUB_KEY|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_CREATE_LINK Registry: HKEY_LOCAL_MACHINE Disposition: REG_CREATED_NEW_KEY Class: SubKey: SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: advapi32	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0068d7c1 0x0040122a	**RegSetValueExW**	Handle: 0x000004b4 Buffer: 1 BufferLength: 4 ValueName: NoAutoUpdate Type: REG_DWORD FullName: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\NoAutoUpdate	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: advapi32	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0068d7a8 0x0040122a	**RegCloseKey**	Handle: 0x000004b4	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0068d7a8 0x0040122a	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:25,034	5280	0x0068d7a8 0x0040122a	**NtDelayExecution**	Milliseconds: 1000	success	0x00000000	
2019-04-18 21:18:26,050	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: kernel32	success	0x00000000	
2019-04-18 21:18:26,050	5280	0x0068d7a8 0x0040122a	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:26,050	5280	0x0068d7a8 0x0040122a	**NtDelayExecution**	Milliseconds: 2000	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: user32	success	0x00000000	1 time
2019-04-18 21:18:28,065	5280	0x0068d7df 0x0040122a	**CreateWindowExW**	Style: 0x00000000 Height: 0 ClassName: zbpnsbtd Width: 0 WindowName: zbpnsbtd y: 0 x: 0	success	0x00000001	
2019-04-18 21:18:28,065	5280	0x0068d7df 0x0040122a	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: user32	success	0x00000000	2 times
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtOpenSection**	DesiredAccess: 0x00000004 ObjectAttributes: \Sessions\1\Windows\ThemeSection	success	0x00000000	

				SectionHandle: 0x000004b0			
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtMapViewOfSection**	Win32Protect: PAGE_READONLY ViewSize: 0x00001000 SectionOffset: 0x0019e0a4 SectionHandle: 0x000004b0 StackPivoted: no ProcessHandle: 0xffffffff BaseAddress: 0x04370000	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtOpenSection**	DesiredAccess: 0x00000004 ObjectAttributes: \Windows\Theme2871853871 SectionHandle: 0x000003b8	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtOpenSection**	DesiredAccess: 0x00000004 ObjectAttributes: \Sessions\1\Windows\Theme3211504610 SectionHandle: 0x000003c0	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtClose**	Handle: 0x000004b0	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtMapViewOfSection**	Win32Protect: PAGE_READONLY ViewSize: 0x000b4000 SectionOffset: 0x0019e72c SectionHandle: 0x000003b8 StackPivoted: no ProcessHandle: 0xffffffff BaseAddress: 0x04ee0000	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtMapViewOfSection**	Win32Protect: PAGE_READONLY ViewSize: 0x00004000 SectionOffset: 0x0019e72c SectionHandle: 0x000003c0 StackPivoted: no ProcessHandle: 0xffffffff BaseAddress: 0x04370000	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**LdrGetDllHandle**	ModuleHandle: 0x77710000 FileName: ntdll.dll	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtCreateMutant**	Handle: 0x000004b0 InitialOwner: 0 MutexName: Local\SM0:5308:168:WilStaging_02	success	0x40000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtWaitForSingleObject**	Status: Infinite Handle: 0x000004b0 Milliseconds: 4294967295	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtWaitForSingleObject**	Handle: 0x000003c8 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtClose**	Handle: 0x000003c8	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtClose**	Handle: 0x000004b0	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtOpenSection**	DesiredAccess: 0x0000000f ObjectAttributes: dwmapi.dll SectionHandle: 0x00000000	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtQueryAttributesFile**	FileName: C:\Windows\System32\dwmapi.dll	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\dwmapi.dll DesiredAccess: FILE_READ_ACCESS|FILE_EXECUTE|SYNCHRONIZE FileHandle: 0x000003c8	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtCreateSection**	ObjectAttributes: DesiredAccess: SECTION_QUERY|SECTION_MAP_READ|SECTION_MAP_WRITE|SECTION_MAP_EXECUTE SectionHandle: 0x000003cc FileHandle: 0x000003c8	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7390b000	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY	success	0x00000000	

				NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000			
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x73909000	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtClose**	Handle: 0x000003cc	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtClose**	Handle: 0x000003c8	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x73909000	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: DDRAW.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D8.DLL	failed	DLL_NOT_FOUND	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D9.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\dwmapi.dll DesiredAccess: READ_CONTROL FileHandle: 0x000003c8	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtClose**	Handle: 0x000003c8	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x73795000	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0069c3bf 0x0068d7df	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x73795000	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0068d7df 0x0040122a	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: user32	success	0x00000000	2 times
2019-04-18 21:18:28,065	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0040122a 0x00000000	**NtOpenSection**	DesiredAccess: 0x0000000f ObjectAttributes: ws2_32.DLL SectionHandle: 0x000003c4	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY	success	0x00000000	

				MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74b6f000			
2019-04-18 21:18:28,065	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00003000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x7782b000	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74b6d000	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0040122a 0x00000000	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x74b6d000	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000003c4	success	0x00000000	
2019-04-18 21:18:28,065	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: DDRAW.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:28,065	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D8.DLL	failed	DLL_NOT_FOUND	
2019-04-18 21:18:28,065	5280	0x0040122a 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x00000000 FileName: D3D9.DLL	failed	DLL_NOT_FOUND	1 time
2019-04-18 21:18:28,065	5280	0x0040122a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\ws2_32.dll DesiredAccess: READ_CONTROL FileHandle: 0x000003c4	success	0x00000000	
2019-04-18 21:18:28,081	5280	0x0040122a 0x00000000	**NtClose**	Handle: 0x000003c4	success	0x00000000	
2019-04-18 21:18:28,081	5280	0x0068d7ad 0x0040122a	**WSAStartup**	VersionRequested: 0x00000101	success	0x00000000	
2019-04-18 21:18:28,081	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	1 time
2019-04-18 21:18:28,362	5280	0x0068d7a8 0x0040122a	**gethostbyname**	Name: ns1.musiczipz.com	failed	0x00000000	
2019-04-18 21:18:28,362	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:28,362	5280	0x0068d7b2 0x0040122a	**socket**	protocol: IPPROTO_TCP socket: 1424 af: AF_INET type: SOCK_STREAM	success	0x00000590	
2019-04-18 21:18:28,362	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:28,362	5280	0x0068d7b2 0x0040122a	**connect**	ip: 255.255.255.255 socket: 1424 port: 0	failed	0xffffffff	
2019-04-18 21:18:28,362	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	

2019-04-18 21:18:28,362	5280	0x0068d7b7 0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READONLY NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READWRITE MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x725af000	success	0x00000000	
2019-04-18 21:18:28,362	5280	0x0068d7b7 0x0040122a	**NtProtectVirtualMemory**	StackPivoted: no OldAccessProtection: PAGE_READWRITE NumberOfBytesProtected: 0x00001000 NewAccessProtection: PAGE_READONLY MemoryType: 0x01000000 ProcessHandle: 0xffffffff BaseAddress: 0x725af000	success	0x00000000	
2019-04-18 21:18:28,362	5280	0x0068d7b7 0x0040122a	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \Device\Afd\AsyncSelectHlp DesiredAccess: GENERIC_READ|GENERIC_WRITE|SYNCHRONIZE ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OPEN_IF FileHandle: 0x00000598 FileAttributes: 0x00000000	success	0x00000000	
2019-04-18 21:18:28,362	5280	0x0068d7b7 0x0040122a	**NtSetInformationFile**	FileInformationClass: FileCompletionInformation HandleName: \Device\Afd FileInformation: \x9c\x05\x00\x00\xc0\xe3Wr FileHandle: 0x00000598	success	0x00000000	
2019-04-18 21:18:28,362	5280	0x0068d7b7 0x0040122a	**NtDeviceIoControlFile**	InputBuffer: \x02\x00\x00\x00\xeeGuw\x01\x00\x00\x00\x00\x00\x00\x00 IoControlCode: IOCTL_AFD_SET_INFO OutputBuffer: FileHandle: 0x00000590	success	0x00000000	
2019-04-18 21:18:28,362	5280	0x0068d7b7 0x0040122a	**CreateThread**	ThreadId: 5944 StartRoutine: 0x7257a160 Parameter: 0x006859d0 CreationFlags: 0x00000000	success	0x000005a4	
2019-04-18 21:18:28,362	5280	0x0068d7b7 0x0040122a	**NtClose**	Handle: 0x000005a4	success	0x00000000	
2019-04-18 21:18:28,362	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	1 time
2019-04-18 21:18:28,362	5944	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer: \xff\xff\xff\xff\xff\xff\xff\x7f\x01\x00\x00\x00\x01\x00a\x00\x90\x05\x00\x009\x00\x00\x00\x00\x00\x00\x00\x02\x00\x00\x00 IoControlCode: IOCTL_AFD_SELECT OutputBuffer: \xff\xff\xff\xff\xff\xff\xff\x7f\x01\x00\x00\x00\x01\x00a\x00\x90\x05\x00\x009\x00\x00\x00\x00\x00\x00\x00\x002\x00\x00\x00\xf0\xd8\xb4F\x00\x0c\x00\x8c\x8c1d\x00\x8c1d\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\xe9\xd8\x8dF\x00 \x00\x888\xbeZr\xd0Yh\x00x\x05\x00\x00\xff\xff\xff\xff\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x80\xc1c\x00\x00\x00\x00\x00\xe2\xd8\x8aF\x00\x0e\x00\x8c\x1c#d\x00\x1c#d\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\xdb\xd8\x83F\x00\x0f\x00\x8c\xbc7d\x00\xbc7d\x00\x00 \x00\x00\x00\x00\x02\x00\x00\x00\x00\x00\x00\x00\x02\x00\x00\x00\x00\x00\x00h\x07h\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x02\x00\x00\x00\x00\x00\x00\x00 FileHandle: 0x00000598	success	0x00000103	
2019-04-18 21:18:28,753	5280	0x0068d7a8 0x0040122a	**gethostbyname**	Name: ns1.musicmixa.net	failed	0x00000000	
2019-04-18 21:18:28,753	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:28,753	5280	0x0068d7b2 0x0040122a	**socket**	protocol: IPPROTO_TCP socket: 1448 af: AF_INET type: SOCK_STREAM	success	0x000005a8	
2019-04-18 21:18:28,753	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:28,753	5280	0x0068d7b2 0x0040122a	**connect**	ip: 255.255.255.255 socket: 1448 port: 0	failed	0xffffffff	

2019-04-18 21:18:28,753	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:28,753	5280	0x0068d7b7 0x0040122a	**NtDeviceIoControlFile**	InputBuffer: \x02\x00\x00\x00\xeeGuw\x01\x00\x00\x00\x00\x00\x00\x00\x00 IoControlCode: IOCTL_AFD_SET_INFO OutputBuffer: FileHandle: 0x000005a8	success	0x00000000	
2019-04-18 21:18:28,753	5944	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer: \xff\xff\xff\xff\xff\xff\xff\x7f\x01\x00\x00\x00\x01\x00\x00\x00\xa8\x05\x00\x009\x00\x00\x00\x06\x00\x00 \x00\x00\x00\x00\x00 IoControlCode: IOCTL_AFD_SELECT OutputBuffer: FileHandle: 0x00000598	success	0x00000103	
2019-04-18 21:18:28,753	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	1 time
2019-04-18 21:18:29,003	5280	0x0068d7a8 0x0040122a	**gethostbyname**	Name: ns1.musicmixa.org	failed	0x00000000	
2019-04-18 21:18:29,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:29,003	5280	0x0068d7b2 0x0040122a	**socket**	protocol: IPPROTO_TCP socket: 1444 af: AF_INET type: SOCK_STREAM	success	0x000005a4	
2019-04-18 21:18:29,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:29,003	5280	0x0068d7b2 0x0040122a	**connect**	ip: 255.255.255.255 socket: 1444 port: 0	failed	0xffffffff	
2019-04-18 21:18:29,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:29,003	5280	0x0068d7b7 0x0040122a	**NtDeviceIoControlFile**	InputBuffer: \x02\x00\x00\x00\xeeGuw\x01\x00\x00\x00\x00\x00\x00\x00\x00 IoControlCode: IOCTL_AFD_SET_INFO OutputBuffer: FileHandle: 0x000005a4	success	0x00000000	
2019-04-18 21:18:29,003	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	1 time
2019-04-18 21:18:29,018	5944	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer: \xff\xff\xff\xff\xff\xff\xff\x7f\x01\x00\x00\x00\x01\x00y\x00\xa4\x05\x00\x009\x00\x00\x00\x00\x003\x002\ x00\x00\x00 IoControlCode: IOCTL_AFD_SELECT OutputBuffer: \xff\xff\xff\xff\xff\xff\xff\x7f\x01\x00\x00\x00\x01\x00y\x00\xa4\x05\x00\x009\x00\x00\x00\x00\x003\x00 2\x00\x00\x00\x95\xd8YF\x00\x19\x00\x8c\xe8\xd9b\x00\xe8\xd0a\x00\xe8\xd9b\x00\x00\x00\x00\x00]v\x0f+\xe9\xc0qA\x 90\x8e\x08\xa6\x11\xb8O\xf6\xff\xff\xff\xff\x00\x00\x00\x00\xe0Uh\x00\x00\x00\x00\x00\x8e\xd8VF\x00\x1a\x00\x8cL4 d\x00L4d\x00\x00\x00\x00\x00\x02\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x87\xd8/F\x00\x1b\x00\x80\x00\x00\x00\x00\x00\x00\x0 0\x00\x8c\xf8\x19\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x001\xf8\x19\x00\x00\x00\x00\x00\x00\x00\x00\x0 0\x00\x00\x00\x00\x10\x00\x00\x00\x00\x00\x00\x00\x00\x80\xd8$F\x00\x1c\x00\x80W\x00s\x002\x00_\x003\x002\x00N\x00u\x 00m\x00H\x00a\x00n\x00d\x00l\x00e\x00B\x00u\x00c\x00k\x00e\x00t\x00s\x00\x00\x00\x00\x00 FileHandle: 0x00000598	success	0x00000103	
2019-04-18 21:18:29,268	5280	0x0068d7a8 0x0040122a	**gethostbyname**	Name: ns1.musicmixb.co	failed	0x00000000	
2019-04-18 21:18:29,268	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:29,268	5280	0x0068d7b2 0x0040122a	**socket**	protocol: IPPROTO_TCP socket: 1452 af: AF_INET type: SOCK_STREAM	success	0x000005ac	
2019-04-18 21:18:29,268	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:29,268	5280	0x0068d7b2 0x0040122a	**connect**	ip: 255.255.255.255 socket: 1452 port: 0	failed	0xffffffff	

2019-04-18 21:18:29,268	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:29,268	5280	0x0068d7b7 0x0040122a	**NtDeviceIoControlFile**	InputBuffer: \x02\x00\x00\x00\xeeGuw\x01\x00\x00\x00\x00\x00\x00\x00 IoControlCode: IOCTL_AFD_SET_INFO OutputBuffer: FileHandle: 0x000005ac	success	0x00000000	
2019-04-18 21:18:29,268	5944	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer: \xff\xff\xff\xff\xff\xff\xff\x7f\x01\x00\x00\x00\x01\x00\x00\x00\xac\x05\x00\x009\x00\x00\x00\x10\x00\x00 \x00\x00\x00\x00\x00 IoControlCode: IOCTL_AFD_SELECT OutputBuffer: FileHandle: 0x00000598	success	0x00000103	
2019-04-18 21:18:29,268	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	1 time
2019-04-18 21:18:29,706	5280	0x0068d7a8 0x0040122a	**gethostbyname**	Name: ns1.musicmixc.com	failed	0x00000000	
2019-04-18 21:18:29,706	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:29,706	5280	0x0068d7b2 0x0040122a	**socket**	protocol: IPPROTO_TCP socket: 1456 af: AF_INET type: SOCK_STREAM	success	0x000005b0	
2019-04-18 21:18:29,706	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:29,706	5280	0x0068d7b2 0x0040122a	**connect**	ip: 255.255.255.255 socket: 1456 port: 0	failed	0xffffffff	
2019-04-18 21:18:29,706	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: ws2_32	success	0x00000000	
2019-04-18 21:18:29,706	5280	0x0068d7b7 0x0040122a	**NtDeviceIoControlFile**	InputBuffer: \x02\x00\x00\x00\xeeGuw\x01\x00\x00\x00\x00\x00\x00\x00 IoControlCode: IOCTL_AFD_SET_INFO OutputBuffer: FileHandle: 0x000005b0	success	0x00000000	
2019-04-18 21:18:29,706	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: user32	success	0x00000000	
2019-04-18 21:18:29,706	5944	0x00000000 0x00000000	**NtDeviceIoControlFile**	InputBuffer: \xff\xff\xff\xff\xff\xff\xff\x7f\x01\x00\x00\x00\x01\x00\x00\x00\xb0\x05\x00\x009\x00\x00\x00\x06\x00\x00 \x00\x00\x00\x00\x00 IoControlCode: IOCTL_AFD_SELECT OutputBuffer: FileHandle: 0x00000598	success	0x00000103	
2019-04-18 21:18:29,706	5280	0x0040122a 0x00000000	**LdrLoadDll**	Flags: 0x00000000 BaseAddress: 0x00000000 FileName: user32	success	0x00000000	
2019-04-18 21:18:38,175	1552	0x00000000 0x00000000	**NtDuplicateObject**	TargetHandle: 0x000005b8 TargetProcessHandle: 0xffffffff Options: DUPLICATE_SAME_ACCESS SourceHandle: 0xfffffffe SourceProcessHandle: 0xffffffff	success	0x00000000	
2019-04-18 21:18:38,175	1552	0x00000000 0x00000000	**NtSetTimerEx**	Status: Skipped Milliseconds: 60000	success	0x00000000	1 time
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x0000040c	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x751b0000 FileName: oleaut32.dll	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x00000410	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x00000120 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Ole\FeatureDevelopmentProperties DesiredAccess: KEY_READ	failed	OBJECT_NAME_NOT_FOUND	

				KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000128 ObjectAttributesName: Software\Microsoft\Ole\FeatureDevelopmentProperties			
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Ole DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000128 ObjectAttributesName: Software\Microsoft\Ole	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft DesiredAccess: KEY_READ KeyHandle: 0x00000410 ObjectAttributesHandle: 0x00000128 ObjectAttributesName: Software\Microsoft	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x000002bc	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x00000124	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtOpenKey**	ObjectAttributes: HKEY_CURRENT_USER DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED KeyHandle: 0x00000124 ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Local Settings DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED KeyHandle: 0x0000040c ObjectAttributesHandle: 0x00000124 ObjectAttributesName: Software\Classes\Local Settings	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x00000124	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x000002bc Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x0000040c	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x00000414	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x0000043c	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtClose**	Handle: 0x00000438	success	0x00000000	
2019-04-18 21:18:54,815	828	0x00000000 0x00000000	**NtClose**	Handle: 0x00000378	success	0x00000000	
2019-04-18 21:18:54,815	7476	0x00000000 0x00000000	**NtTerminateThread**	ExitStatus: 0x00000000 ThreadHandle: 0x00000000	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**LdrGetDllHandle**	ModuleHandle: 0x751b0000 FileName: oleaut32.dll	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x00000498	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x00000494	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtWaitForSingleObject**	Handle: 0x00000120 Milliseconds: 0	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Ole\FeatureDevelopmentProperties DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000128 ObjectAttributesName: Software\Microsoft\Ole\FeatureDevelopmentProperties	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Ole DesiredAccess: KEY_READ KeyHandle: 0x00000000 ObjectAttributesHandle: 0x00000128 ObjectAttributesName: Software\Microsoft\Ole	failed	OBJECT_NAME_NOT_FOUND	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft DesiredAccess: KEY_READ	success	0x00000000	

				KeyHandle: 0x00000494 ObjectAttributesHandle: 0x00000128 ObjectAttributesName: Software\Microsoft			
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x00000410	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x000002bc	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtOpenKey**	ObjectAttributes: HKEY_CURRENT_USER DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED KeyHandle: 0x000002bc ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\USER\S-1-5-21-2035269069-1835038330-1888751347-500	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtOpenKeyEx**	ObjectAttributes: HKEY_CURRENT_USER\Software\Classes\Local Settings DesiredAccess:KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|KEY_WOW64_64KEY|STANDARD_RIGHTS_REQUIRED KeyHandle: 0x00000498 ObjectAttributesHandle: 0x000002bc ObjectAttributesName: Software\Classes\Local Settings	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x000002bc	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**GetSystemTimeAsFileTime**		success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtWaitForSingleObject**	Status: Small log limit reached	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x00000498	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x000004ac	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x000004a4	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtClose**	Handle: 0x000004a0	success	0x00000000	
2019-04-18 21:18:54,893	1044	0x00000000 0x00000000	**NtTerminateThread**	ExitStatus: 0x00000000 ThreadHandle: 0x00000000	success	0x00000000	
2019-04-18 21:19:04,909	1552	0x00000000 0x00000000	**NtSetTimerEx**	Status: Skipped Milliseconds: 60000	success	0x00000000	1 time
2019-04-18 21:19:19,503	7796	0x00000000 0x00000000	**NtTerminateThread**	ExitStatus: 0x00000000 ThreadHandle: 0x00000000	success	0x00000000	1 time
2019-04-18 21:19:24,800	828	0x00000000 0x00000000	**NtClose**	Handle: 0x00000594	success	0x00000000	
2019-04-18 21:19:31,643	1552	0x00000000 0x00000000	**NtSetTimerEx**	Status: Skipped Milliseconds: 60000	success	0x00000000	4 times
2019-04-18 21:20:38,550	1552	0x00000000 0x00000000	**NtClose**	Handle: 0x00000408	success	0x00000000	
2019-04-18 21:20:38,550	1552	0x00000000 0x00000000	**NtSetTimerEx**	Status: Skipped Milliseconds: 30000	success	0x00000000	
2019-04-18 21:20:55,190	828	0x00000000 0x00000000	**NtClose**	Handle: 0x00000444	success	0x00000000	
2019-04-18 21:21:17,925	1552	0x00000000 0x00000000	**NtClose**	Handle: 0x00000408	success	0x00000000	
2019-04-18 21:21:17,925	1552	0x00000000 0x00000000	**NtClose**	Handle: 0x000003f8	success	0x00000000	
2019-04-18 21:21:17,925	1552	0x00000000 0x00000000	**NtClose**	Handle: 0x000005b8	success	0x00000000	
2019-04-18 21:21:17,925	1552	0x00000000 0x00000000	**NtClose**	Handle: 0x000005b4	success	0x00000000	
2019-04-18 21:21:17,925	1552	0x00000000 0x00000000	**NtTerminateThread**	ExitStatus: 0x00000000 ThreadHandle: 0x00000000	success	0x00000000	