Time	TID	Caller	API	Arguments	Status	Return	Repeated
2018-10-31 13:51:24,203	5824	0x00408b26 0x0040987e	**NtQueryAttributesFile**	FileName: C:\Users\Administrator\AppData\Local\Temp\CRYPTSP.dll	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,203	5824	0x00408b26 0x0040987e	**NtQueryAttributesFile**	FileName: C:\Windows\System32\cryptsp.dll	success	0x00000000	
2018-10-31 13:51:24,203	5824	0x00408b26 0x0040987e	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\cryptsp.dll DesiredAccess: FILE_READ_ACCESS|FILE_EXECUTE|SYNCHRONIZE FileHandle: 0x00000268	success	0x00000000	
2018-10-31 13:51:24,203	5824	0x00408b26 0x0040987e	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\cryptsp.dll DesiredAccess: READ_CONTROL FileHandle: 0x00000268	success	0x00000000	
2018-10-31 13:51:24,218	5824	0x004057d9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: C:\ DesiredAccess: SYNCHRONIZE FileHandle: 0x0000026c	success	0x00000000	
2018-10-31 13:51:24,218	5824	0x004057d9 0x00000000	**NtQueryInformationFile**	FileInformationClass: FileNameInformation HandleName: C:\ FileInformation: \x02\x00\x00\x00\\x00 FileHandle: 0x0000026c	success	0x00000000	
2018-10-31 13:51:24,218	5824	0x00405dd9 0x00000000	**GetFileVersionInfoSizeW**	PathName: C:\Users\Administrator\AppData\Local\Temp\tdbanksetup.exe	success	0x000006e4	
2018-10-31 13:51:24,218	5824	0x00405df9 0x00000000	**GetFileVersionInfoW**	PathName: C:\Users\Administrator\AppData\Local\Temp\tdbanksetup.exe	success	0x00000001	
2018-10-31 13:51:24,218	5824	0x004058a0 0xfffffffe	**SHGetFolderPathW**	Path: C:\WINDOWS Folder: CSIDL_WINDOWS	success	0x00000000	
2018-10-31 13:51:24,218	5824	0x004058f2 0xfffffffe	**GetVolumeNameForVolumeMountPoint W**	VolumeMountPoint: C:\WINDOWS\ VolumeName:	failed	0x00000000	
2018-10-31 13:51:24,218	5824	0x004058f2 0xfffffffe	**GetVolumeNameForVolumeMountPoint W**	VolumeMountPoint: C:\ VolumeName: \\?\Volume{f1a163df-0000-0000-0000-501f00000000}\	success	0x00000001	
2018-10-31 13:51:24,218	5824	0x004089c9 0x0040987e	**SHGetFolderPathW**	Path: C:\Users\Administrator\AppData\Roaming Folder: CSIDL_APPDATA	success	0x00000000	
2018-10-31 13:51:24,218	5824	0x004069c5 0x00000000	**NtCreateFile**	ShareAccess: 0 FileName: C:\Users\Administrator\AppData\Local\Temp\tdbanksetup.exe DesiredAccess: FILE_READ_EA ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x000002cc FileAttributes: FILE_ATTRIBUTE_NORMAL	success	0x00000000	
2018-10-31 13:51:24,218	5824	0x00401a2d 0x00000000	**NtQueryAttributesFile**	FileName: C:\Users\Administrator\AppData\Local\Temp\tdbanksetup.dbg	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x00401591 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: C:\popupkiller.exe DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x00000000 FileAttributes: 0x00000000	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x00401591 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: C:\stimulator.exe DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x00000000 FileAttributes: 0x00000000	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x00401591 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: C:\TOOLS\execute.exe DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x00000000 FileAttributes: 0x00000000	failed	OBJECT_PATH_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x004016dc 0x00000000	**NtQueryAttributesFile**	FileName: C:\Users\Administrator\AppData\Local\Temp\SbieDll.dll	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x004016dc 0x00000000	**NtQueryAttributesFile**	FileName: C:\Windows\System32\SbieDll.dll	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x004016dc 0x00000000	**NtQueryAttributesFile**	FileName: C:\Windows\System\SbieDll.dll	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x004016dc	**NtQueryAttributesFile**	FileName: C:\Windows\SbieDll.dll	failed	OBJECT_NAME_NOT_FOUND	

		0x00000000					
2018-10-31 13:51:24,218	5824	0x004016dc 0x00000000	**NtQueryAttributesFile**	FileName: C:\Users\Administrator\AppData\Local\Temp\SbieDll.dll	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x004016dc 0x00000000	**NtQueryAttributesFile**	FileName: C:\Python27\SbieDll.dll	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x004016dc 0x00000000	**NtQueryAttributesFile**	FileName: C:\Python27\Scripts\SbieDll.dll	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x004016dc 0x00000000	**NtQueryAttributesFile**	FileName: C:\Program Files (x86)\Common Files\Oracle\Java\javapath\SbieDll.dll	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x004016dc 0x00000000	**NtQueryAttributesFile**	FileName: C:\Windows\System32\SbieDll.dll	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x004016dc 0x00000000	**NtQueryAttributesFile**	FileName: C:\Windows\SbieDll.dll	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x004016dc 0x00000000	**NtQueryAttributesFile**	FileName: C:\Windows\System32\wbem\SbieDll.dll	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x004016dc 0x00000000	**NtQueryAttributesFile**	FileName: C:\Windows\System32\WindowsPowerShell\v1.0\SbieDll.dll	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x004016dc 0x00000000	**NtQueryAttributesFile**	FileName: C:\Windows\System32\OpenSSH\SbieDll.dll	failed	OBJECT_PATH_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x004016dc 0x00000000	**NtQueryAttributesFile**	FileName: C:\Users\Administrator\AppData\Local\Microsoft\WindowsApps\SbieDll.dll	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,218	5824	0x00401591 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\NPF_NdisWanIp DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x00000000 FileAttributes: 0x00000000	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,249	5824	0x00401591 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\REGVXG DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x00000000 FileAttributes: 0x00000000	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,249	5824	0x00401591 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\FILEVXG DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x00000000 FileAttributes: 0x00000000	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,249	5824	0x00401591 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\REGSYS DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x00000000 FileAttributes: 0x00000000	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,249	5824	0x00401591 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\FILEM DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x00000000 FileAttributes: 0x00000000	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,249	5824	0x00401591 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE FileName: \??\TRW DesiredAccess: FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x00000000 FileAttributes: 0x00000000	failed	OBJECT_NAME_NOT_FOUND	
2018-10-31 13:51:24,249	5824	0x0040b8f6 0x00000000	**NtQueryAttributesFile**	FileName: C:\Users\Administrator\AppData\Roaming	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE	success	0x00000000	

				FileHandle: 0x00000264			
2018-10-31 13:51:24,249	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000264	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002c8	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002c8	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002bc	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000264	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002bc	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002c8	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002bc	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Credentials\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002c8	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002c8	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\	success	0x00000000	

				DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4			
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\ImplicitAppShortcuts\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\UserData\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\UserData\Low\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\MMC\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002c8	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002c8	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\Connections\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\Connections\Cm\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\Connections_hiddencm\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002c8	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\S-1-5-21-2035269069-1835038330-1888751347-500\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002c8	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	

2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Vault\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002c8	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002c8	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\AccountPictures\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,249	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\CloudStore\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Network Shortcuts\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Printer Shortcuts\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002e0	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002e4	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE	success	0x00000000	

		0x0055005c		FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002e4			
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002e4	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002e4	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002e4	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002e4	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002e4	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Templates\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d0	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002e0	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x0040b713 0x0055005c	**NtCreateFile**	ShareAccess: 0 FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\Command Prompt.kup DesiredAccess: GENERIC_READ|GENERIC_WRITE|FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OVERWRITE_IF FileHandle: 0x00000264 FileAttributes: FILE_ATTRIBUTE_NORMAL	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x0040b732 0x0055005c	**NtQueryAttributesFile**	FileName: C:\Windows\System32\ntmarta.dll	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x0040b732 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\ntmarta.dll DesiredAccess: FILE_READ_ACCESS|FILE_EXECUTE|SYNCHRONIZE FileHandle: 0x00000264	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x0040b732 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\System32\ntmarta.dll DesiredAccess: READ_CONTROL FileHandle: 0x00000264	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x0040515d 0x0040b732	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\Command Prompt.kup DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL|WRITE_OWNER FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x0040515d 0x0040b732	**NtQueryInformationFile**	FileInformationClass: FileBasicInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\Command Prompt.kup FileInformation: \x02*4n\x18q\xd4\x01\x02*4n\x18q\xd4\x01\x02*4n\x18q\xd4\x01\x02*4n\x18q\xd4\x01 \x00\x00\x00\x00\x00\x00\x00	success	0x00000000	

				FileHandle: 0x000002f0			
2018-10-31 13:51:24,265	5824	0x0040515d 0x0040b732	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: READ_CONTROL FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x0040515d 0x0040b732	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player FileInformation: FileHandle: 0x000002f8	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,265	5824	0x0040515d 0x0040b732	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\Command Prompt.kup FileInformation: FileHandle: 0x000002f0	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,265	5824	0x00404ee7 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\Command Prompt.kup DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x00404ee7 0x00000000	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\Command Prompt.kup FileInformation: FileHandle: 0x000002f0	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,265	5824	0x00404ee7 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: READ_CONTROL FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x00404ee7 0x00000000	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player FileInformation: FileHandle: 0x000002f4	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,265	5824	0x00404ee7 0x00000000	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\Command Prompt.kup FileInformation: FileHandle: 0x000002f0	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,265	5824	0x00404ee7 0x00000000	**NtQueryInformationFile**	FileInformationClass: FileBasicInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\Command Prompt.kup FileInformation: \x02*4n\x18q\xd4\x01\x02*4n\x18q\xd4\x01\x02*4n\x18q\xd4\x01\x02*4n\x18q\xd4\x01\x02*4n\x18q\xd4\x01 \x00\x00\x00\x00\x00\x00\x00\x00 FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,265	5824	0x00404f41 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\Command Prompt.kup DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL|WRITE_DAC FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x00404f41 0x00000000	**NtQueryInformationFile**	FileInformationClass: FileBasicInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\Command Prompt.kup FileInformation: \x02*4n\x18q\xd4\x01\x02*4n\x18q\xd4\x01\x02*4n\x18q\xd4\x01\x02*4n\x18q\xd4\x01\x02*4n\x18q\xd4\x01 \x00\x00\x00\x00\x00\x00\x00\x00 FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x00404f41 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: READ_CONTROL FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x00404f41 0x00000000	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player FileInformation: FileHandle: 0x000002f8	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,281	5824	0x00404f41 0x00000000	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\Command Prompt.kup FileInformation: FileHandle: 0x000002f0	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,281	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f0	success	0x00000000	

2018-10-31 13:51:24,281	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x00405205 0x0040b4b6	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming FileInformation: FileHandle: 0x000002f0	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,281	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x00405205 0x0040b4b6	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe FileInformation: FileHandle: 0x000002f4	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,281	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x00405205 0x0040b4b6	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player FileInformation: FileHandle: 0x000002d8	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,281	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x00405205 0x0040b4b6	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache FileInformation: FileHandle: 0x000002dc	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,281	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x00405205	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation	failed	INVALID_PARAMETER	

		0x0040b4b6		HandleName: C:\Users\Administrator\AppData\Roaming\Microsoft FileInformation: FileHandle: 0x000002f8			
2018-10-31 13:51:24,281	5824	0x004065e3 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f0	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Credentials\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\ImplicitAppShortcuts\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000300	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\UserData\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\UserData\Low\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\MMC\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	**success**	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE	**success**	0x00000000	

		0x0055005c		FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\Connections\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc			
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\Connections\Cm\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\Connections_hiddencm\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\S-1-5-21-2035269069-1835038330-1888751347-500\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,281	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Vault\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\AccountPictures\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\CloudStore\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\NetworkShortcuts\	success	0x00000000	

				DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8			
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Printer Shortcuts\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000300	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000300	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000300	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000300	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000300	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE	success	0x00000000	

		0x0055005c		FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Templates \ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc			
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\Ca chedFiles\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x0040b713 0x0055005c	**NtCreateFile**	ShareAccess: 0 FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\Desktop.gow DesiredAccess: GENERIC_READ|GENERIC_WRITE|FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OVERWRITE_IF FileHandle: 0x000002f0 FileAttributes: FILE_ATTRIBUTE_NORMAL	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x00405205 0x0040b4b6	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming FileInformation: FileHandle: 0x000002f0	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,296	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x00405205 0x0040b4b6	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe FileInformation: FileHandle: 0x000002d4	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,296	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,296	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x00405205 0x0040b4b6	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player FileInformation: FileHandle: 0x000002d8	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,312	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x0040b49a	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE	success	0x00000000	

		0x00000000		FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8			
2018-10-31 13:51:24,312	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x00405205 0x0040b4b6	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache FileInformation: FileHandle: 0x000002f8	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,312	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x00405205 0x0040b4b6	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Microsoft FileInformation: FileHandle: 0x000002d4	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,312	5824	0x004065e3 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Credentials\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE	success	0x00000000	

		0x0055005c		FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\ImplicitAppShortcuts\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc			
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\UserData\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\UserData\Low\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\MMC\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\Connections\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\Connections\Cm\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\Connections_hiddencm\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\S-1-5-21-2035269069-1835038330-1888751347-500\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs\	success	0x00000000	

				DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8			
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Vault\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\AccountPictures\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\CloudStore\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Network Shortcuts\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Printer Shortcuts\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,312	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,328	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,328	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000300	success	0x00000000	
2018-10-31 13:51:24,328	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000304	success	0x00000000	
2018-10-31 13:51:24,328	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000308	success	0x00000000	
2018-10-31 13:51:24,328	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE	success	0x00000000	

				FileHandle: 0x00000308			
2018-10-31 13:51:24,328	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000308	success	0x00000000	
2018-10-31 13:51:24,328	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000308	success	0x00000000	
2018-10-31 13:51:24,328	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000308	success	0x00000000	
2018-10-31 13:51:24,328	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000308	success	0x00000000	
2018-10-31 13:51:24,328	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000308	success	0x00000000	
2018-10-31 13:51:24,328	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Templates\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000300	success	0x00000000	
2018-10-31 13:51:24,328	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000300	success	0x00000000	
2018-10-31 13:51:24,328	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x00000304	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x0040b713 0x0055005c	**NtCreateFile**	ShareAccess: 0 FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\computer.xik DesiredAccess: GENERIC_READ|GENERIC_WRITE|FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OVERWRITE_IF FileHandle: 0x000002f0 FileAttributes: FILE_ATTRIBUTE_NORMAL	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x00405205 0x0040b4b6	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming FileInformation: FileHandle: 0x000002f0	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,343	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL	success	0x00000000	

				FileHandle: 0x000002f4			
2018-10-31 13:51:24,343	5824	0x00405205 0x0040b4b6	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe FileInformation: FileHandle: 0x000002f4	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,343	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x00405205 0x0040b4b6	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player FileInformation: FileHandle: 0x000002dc	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,343	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x00405205 0x0040b4b6	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache FileInformation: FileHandle: 0x000002f8	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,343	5824	0x0040b5a9 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x0040b49a 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x00405205 0x0040b4b6	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft DesiredAccess: FILE_READ_ATTRIBUTES|READ_CONTROL FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,343	5824	0x00405205 0x0040b4b6	**NtQueryInformationFile**	FileInformationClass: FileReplaceCompletionInformation HandleName: C:\Users\Administrator\AppData\Roaming\Microsoft FileInformation: FileHandle: 0x000002f8	failed	INVALID_PARAMETER	
2018-10-31 13:51:24,343	5824	0x004065e3 0x00000000	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\NativeCache\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE	success	0x00000000	

				FileHandle: 0x000002f4			
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Credentials\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\ImplicitAppShortcuts\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\UserData\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\UserData\Low\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\MMC\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\Connections\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\Connections\Cm\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Network\Connections_hiddencm\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE	success	0x00000000	

		0x0055005c		FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\S-1-5-21-2035269069-1835038330-1888751347-500\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4			
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Vault\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002fc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\AccountPictures\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\CloudStore\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\NetworkShortcuts\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\PrinterShortcuts\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE	success	0x00000000	

		0x0055005c		FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc			
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002d4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Templates\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002f4	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x004065e3 0x0055005c	**NtOpenFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE FileName: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\ DesiredAccess: FILE_READ_ACCESS|SYNCHRONIZE FileHandle: 0x000002dc	success	0x00000000	
2018-10-31 13:51:24,359	5824	0x0040b713 0x0055005c	**NtCreateFile**	ShareAccess: 0 FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\f01b4d95cf55d32a.exe DesiredAccess: GENERIC_READ|GENERIC_WRITE|FILE_READ_ATTRIBUTES|SYNCHRONIZE	success	0x00000000	

				ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OVERWRITE_IF FileHandle: 0x000002f0 FileAttributes: FILE_ATTRIBUTE_NORMAL			
2018-10-31 13:51:24,374	5824	0x004058a0 0x00000000	**SHGetFolderPathW**	Path: C:\WINDOWS Folder: CSIDL_WINDOWS	success	0x00000000	
2018-10-31 13:51:24,374	5824	0x004058f2 0x00000000	**GetVolumeNameForVolumeMountPointW**	VolumeMountPoint: C:\WINDOWS\ VolumeName:	failed	0x00000000	
2018-10-31 13:51:24,374	5824	0x004058f2 0x00000000	**GetVolumeNameForVolumeMountPointW**	VolumeMountPoint: C:\ VolumeName: \\?\Volume{f1a163df-0000-0000-0000-501f00000000}\	success	0x00000001	
2018-10-31 13:51:24,374	5824	0x0040607b 0x0040b84a	**NtCreateFile**	ShareAccess: FILE_SHARE_READ FileName: C:\Users\Administrator\AppData\Local\Temp\tdbanksetup.exe DesiredAccess: GENERIC_READ|FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x000002f0 FileAttributes: 0x00000000	success	0x00000000	
2018-10-31 13:51:24,374	5824	0x0040608e 0x0040b84a	**NtQueryInformationFile**	FileInformationClass: FileStandardInformation HandleName: C:\Users\Administrator\AppData\Local\Temp\tdbanksetup.exe FileInformation:\x000\x02\x00\x00\x00\x00\x00\x000\x02\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00 FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,374	5824	0x004060ce 0x0040b84a	**NtReadFile**	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\x18\x01\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\x1c<\xd2\x07X]\xbcTX]\xbcTX]\xbcT#A\xb0T^]\xbcT7B\xb6TS]\xbcT7B\xb8T[]\xbcT7B\xb7TZ]\xbcT\xdbA\xb2TZ]\xbcT\x82~\xa0TY]\xbcT&\x7f\xa1TY]\xbcTk\x7f\x99T^]\xbcT&\x7f\xa0T\]\xbcT\xb0B\xb7TY]\xbcTX]\xbdT\xc3]\xbcT:B\xafTV]\xbcT\x0c~\x8dT5]\xbcT\x9f[\xbaTY]\xbcT HandleName: C:\Users\Administrator\AppData\Local\Temp\tdbanksetup.exe Length: 143360 FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,374	5824	0x0040600c 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\f01b4d95cf55d32a.exe DesiredAccess: GENERIC_WRITE|FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_OVERWRITE_IF FileHandle: 0x000002f8 FileAttributes: FILE_ATTRIBUTE_NORMAL	success	0x00000000	
2018-10-31 13:51:24,374	5824	0x0040602f 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\x00\x18\x01\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\x1c<\xd2\x07X]\xbcTX]\xbcTX]\xbcT#A\xb0T^]\xbcT7B\xb6TS]\xbcT7B\xb8T[]\xbcT7B\xb7TZ]\xbcT\xdbA\xb2TZ]\xbcT\x82~\xa0TY]\xbcT&\x7f\xa1TY]\xbcTk\x7f\x99T^]\xbcT&\x7f\xa0T\]\xbcT\xb0B\xb7TY]\xbcTX]\xbdT\xc3]\xbcT:B\xafTV]\xbcT\x0c~\x8dT5]\xbcT\x9f[\xbaTY]\xbcT HandleName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\f01b4d95cf55d32a.exe Length: 143360 FileHandle: 0x000002f8	success	0x00000000	
2018-10-31 13:51:24,390	5824	0x004068a2 0x00000000	**NtCreateFile**	ShareAccess: 0 FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\f01b4d95cf55d32a.exe DesiredAccess: FILE_WRITE_EA ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x000002f0 FileAttributes: FILE_ATTRIBUTE_NORMAL	success	0x00000000	
2018-10-31 13:51:24,390	5824	0x00406449	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_WRITE|FILE_SHARE_DELETE	success	0x00000000	

		0x00000000		FileName: C:\Users\Administrator\AppData\Roaming DesiredAccess: GENERIC_READ|FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x000002f0 FileAttributes: 0x00000000			
2018-10-31 13:51:24,390	5824	0x0040645d 0x00000000	**NtQueryInformationFile**	FileInformationClass: FileBasicInformation HandleName: C:\Users\Administrator\AppData\Roaming FileInformation:\x06[\xb1\xbf\xf7p\xd4\x01\xe2\xbc\xff\xc0\xf7p\xd4\x01\xe2\xbc \xff\xc0\xf7p\xd4\x01\xe2\xbc\xff\xc0\xf7p\xd4\x01\x10\x00\x00\x00\x00\x00 \x00\x00 FileHandle: 0x000002f0	success	0x00000000	
2018-10-31 13:51:24,390	5824	0x0040476a 0x004047e5	**NtQueryAttributesFile**	FileName: C:\Users\Administrator\AppData\Roaming\Adobe\Flash Player\f01b4d95cf55d32a.exe	success	0x00000000	1 time
2018-10-31 13:51:24,390	5824	0x0040476a 0x004047e5	**NtQueryAttributesFile**	FileName: C:\Users\Administrator\AppData\Roaming	success	0x00000000	
2018-10-31 13:51:24,421	5824	0x0040476a 0x004047e5	**NtCreateFile**	ShareAccess: FILE_SHARE_READ|FILE_SHARE_DELETE FileName: C:\Windows\apppatch\sysmain.sdb DesiredAccess: GENERIC_READ|FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_OPEN FileHandle: 0x000002dc FileAttributes: FILE_ATTRIBUTE_NORMAL	success	0x00000000	
2018-10-31 13:51:24,421	5824	0x0040476a 0x004047e5	**NtQueryInformationFile**	FileInformationClass: FileStandardInformation HandleName: C:\Windows\apppatch\sysmain.sdb FileInformation: \x00\x80<\x00\x00\x00\x00\x00\xb8~<\x00\x00\x00\x00\x00\x02\x0 0\x00\x00\x00\x00\x00\x00 FileHandle: 0x000002dc	success	0x00000000	1 time
2018-10-31 13:51:24,687	5824	0x0040600c 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ FileName: C:\Users\Administrator\AppData\Local\Temp\updefeb9707.bat DesiredAccess: GENERIC_WRITE|FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: no StackPivoted: no CreateDisposition: FILE_OVERWRITE_IF FileHandle: 0x000002cc FileAttributes: FILE_ATTRIBUTE_NORMAL	success	0x00000000	
2018-10-31 13:51:24,687	5824	0x0040600c 0x00000000	**NtCreateFile**	ShareAccess: FILE_SHARE_READ FileName: C:\Users\Administrator\AppData\Local\Temp\updefeb9707.bat DesiredAccess: GENERIC_WRITE|FILE_READ_ATTRIBUTES|SYNCHRONIZE ExistedBefore: yes StackPivoted: no CreateDisposition: FILE_OVERWRITE_IF FileHandle: 0x000002cc FileAttributes: FILE_ATTRIBUTE_NORMAL	success	0x00000000	
2018-10-31 13:51:24,687	5824	0x0040602f 0x00000000	**NtWriteFile**	Buffer: @echo off :d del /F /Q "C:\Users\ADMINI~1\AppData\Local\Temp\tdbanksetup.exe" if exist "C:\Users\ADMINI~1\AppData\Local\Temp\tdbanksetup.exe" goto d del /F "C:\Users\ADMINI~1\AppData\Local\Temp\updefeb9707.bat" HandleName: C:\Users\Administrator\AppData\Local\Temp\updefeb9707.bat Length: 216 FileHandle: 0x000002cc	success	0x00000000	
2018-10-31 13:51:24,718	5824	0x0040476a 0x004047e5	**NtQueryAttributesFile**	FileName: C:\Windows\System32\cmd.exe	success	0x00000000	1 time

Back to the top