

Sandbox Analysis Report

Analysis Overview

Generated time:	2023/01/09 16:14:05 +00:00					
Submitter:	Manual Submission	Manual Submission				
Overall risk level	High risk The object exhib	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	MSIL Portable executable 1.1 - GABOR 08408 SHEET-LATVIA.exe 2798A02A2A853DC16CABF2A062BC4E3069A6F0EA				
	Empty file	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	F4F52BE1186C93ED5C7C927D9E59439BFAD548C995DA9203AC690BDC921D2E B4
MD5	C7C86B69E8A0E5534FBA8F1036FB5C7C
TLSH	-
Size	693614 byte(s)

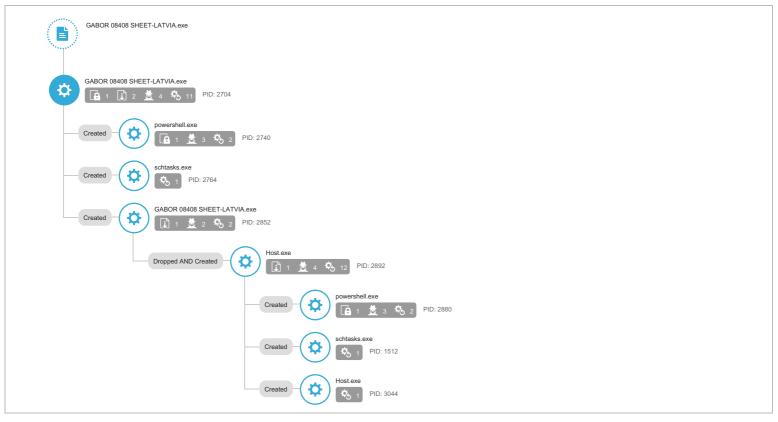
Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

▼ 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	F521274E6C6A1EBACEA6C13874170458C75199B5E61C3768B7F2DCFAC80975C
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

 $\ensuremath{\texttt{©}}$ ATT&CKTM is a trademark of The MITRE Corporation.

▼ 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%lsystem32\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%InstallHost.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-MpPr eference -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe"
Executes dropped file		%TEMP%ltmp1B0.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.lmp"
Executes dropped file	•	File: %TEMP%\tmp180.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp180.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\\$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\\$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\iHost.exe
Creates process in Application Data folder		Process ID: 2892 Image Path: %APPDATA%\InstalliHost.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/MFEwTzBNMEswSTAJB gUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh% 2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7i90 VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk		GABOR 08408 SHEET-LATVIA.exe
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?203 09cde9dfbf0f1	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	2798A02A2A853DC16CABF2A062BC4E3069 A6F0EA
safUcOGLqdWC.exe	Low	TROJ_GEN.R002C0DA723	Drops probable malware	-	742400	2798A02A2A853DC16CABF2A062BC4E3069 A6F0EA
d93f411851d7c929.customDestin ations-ms	No risk	-	-	-	8016	9564EA6257EC40891EC380EF872B2E959A8 DA893
d93f411851d7c929.customDestin ations-ms~RF1c91d7.TMP	No risk	-	-	-	8016	9564EA6257EC40891EC380EF872B2E959A8 DA893
d93f411851d7c929.customDestin ations-ms~RF1c7baf.TMP	No risk	-	-	-	8016	138BBB6356079FC92C29F1B6FB07E4CBE4 8E76F3
1927IGMTQKEP0GP31R1S.temp	No risk	-	-	-	8016	9564EA6257EC40891EC380EF872B2E959A8 DA893
9QC1S46Q8PIM9RKWJ8WZ.tem	No risk	-	-	-	8016	9564EA6257EC40891EC380EF872B2E959A9
tmp1B0.tmp	No risk	-	-	-	1616	71BC48F8D595E94581DB0B2087D33860FF 2C9A7
safUcOGLqdW	No risk	-	-	-	3326	39C51BC9AFC1E9B42A561CD8F8F6EF030 ⁻¹ 148F78
tmp1680.tmp	No risk	-	-	-	1616	71BC48F8D595E94581DB0B2087D33860FF8

▼ Suspicious Objects

Туре	Object	Risk Level
File (SHA1)	2798A02A2A853DC16CABF2A062BC4E3069A6F0EA	High

▼ Analysis

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		
Detection	Global Detections: 0 Threat Characteristic: Uses suspicious packer		
Sociality	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, 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\t^*, 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: (H4sIAAAAAAAAAACAO29B2AcSZYJJi9tynt/SvVK1+B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVm VdZhZAzO2dvPfee++999577733ujudTif33/8/XGZkAWz2zkra) Return: 1F8B08000000000		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: (VHJhbnNhY3Rpb25hbEIP) 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%IGABOR 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: (PD94bWwgdmVyc2lvbj0iMS4wliBlbmNvZGluZz0iVVRGLTE2lj8+CjxUYXNrlHZlcnNpb249ljEuMilgeG1 sbnM9lmh0dHA6Ly9zY2hlbWFzLm1pY3Jvc29mdC5jb20v) 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 Call System API	API Name: evtchann.SendEvent Args: (e), pid[2740], ppid[2704) Return: 1 API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM	2704 2704
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#000000000100000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\) Return: 3	2704
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6(6e6963)#000000006500000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\) 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\ve., "\windir\%\System32\WindowsPowerShell\v1.0\powershell\v2.0\powershell	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-MpPref erence -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: ? API Name: outchans SendEught Args: (a) pid(2764) poid(2704) Return: 1	2704
Call System API Detection	API Name: evtchann.SendEvent Args: (e), pid[2764], ppid[2704) Return: 1 Threat Characteristic: Creates process in system directory Process ID: 2740	2704
Call Process API	Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\safUcOGLqdWC.exe API Name: CreateProcessW Args: (2704
Detection	TEMP%\tmp180.tmp*, , , , %WorkingDir%, SW_HIDE, Process:2764: %windir%\System32\schtasks.exe) Return: 1 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.tm p"	
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\tmp180.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp180.tm	

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
		2704	2740
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3		
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\(\Lambda\) Return: 3	2704	2740
Call System API	API Name: GetDriveTypeW Args: (C\(\lambda\) 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
		2704	2740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		
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-ROM2.5+#5&1c1d869a&0&1.1.0#[53f5630d-b6bf-11d0-94f	2704	2740
Coll Contact ADI	2-00a0c91efb8b)\\) Return: 5	0704	0740
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}#000000000100000#[53f5630d-b6bf-11d0-94f2-00a0 c91efb8b]\) \Return: 3	2704	2740
0.110.1.401		0704	0740
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#000000006500000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\) \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\WindowsPowerShelllv1.0\) 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%IMicrosoft\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		2.01	27.10
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		
2.02	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		
	Threat Characteristic: Creates process in system directory Process ID: 2764		
Detection	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp		
	Threat Characteristic: Creates process in system directory Process ID: 2764		
Detection	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup		2704
Detection	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN		2704
Detection Detection Add File	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML		2704
Detection Detection Add File	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup		2704
Detection Add File Detection	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\safUcOGLqdWC ### Windir%\system32\Tasks\Updates\safUcOGLqdWC ####################################		
Detection Detection Add File Detection Delete File	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\safUcOGLqdWC Path: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2704		
Detection Detection Add File Detection Delete File	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\safUcOGLqdWC Path: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2704 File: %TEMP%\tmp180.tmp		
Detection Detection Add File Detection Delete File Detection	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\safUcOGLqdWC Path: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2704 File: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML		2704
Detection Detection Add File Detection Delete File Detection Call System API	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\ischtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\safUcOGLqdWC Path: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2704 File: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0		2704 2704
Detection Detection Add File Detection Delete File Detection	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%\System32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\System32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\System32\Tasks\Updates\safUcOGLqdWC Path: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2704 File: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, , , , , CREATE_SUSPENDED, , , , Process:2852:%WorkingDir%\GA		2704
Detection Detection Add File Detection Delete File Detection Call System API Call Process API	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windif% System32 schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\safUcOGLqdWC Path: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2704 File: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, , , , , CREATE_SUSPENDED, , , , Process:2852:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, , , , , CREATE_SUSPENDED, , , , Process:2852:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe,) Return: 1		2704 2704
Detection Detection Add File Detection Delete File Detection Call System API	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%\System32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\System32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\System32\Tasks\Updates\safUcOGLqdWC Path: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2704 File: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, , , , , CREATE_SUSPENDED, , , , Process:2852:%WorkingDir%\GA BOR 08408 SHEET-LATVIA.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection		2704
Detection Detection Add File Detection Delete File Detection Call System API Call Process API	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windif% System32 schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\safUcOGLqdWC Path: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2704 File: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, , , , , CREATE_SUSPENDED, , , , Process:2852:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, , , , , CREATE_SUSPENDED, , , , Process:2852:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe,) Return: 1		2704 2704
Detection Detection Add File Detection Delete File Detection Call System API Call Process API	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%\System32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\System32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\System32\Tasks\Updates\safUcOGLqdWC Path: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2704 File: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, , , , , CREATE_SUSPENDED, , , , Process:2852:%WorkingDir%\GA BOR 08408 SHEET-LATVIA.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2704 Injected API: SetThreadContext Target Process ID: 2852		2704
Detection Detection Add File Detection Delete File Detection Call System API Call Process API	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%iSystem32lschtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%isystem32lTasksiUpdates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%isystem32lTasksiUpdates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%isystem32lTasksiUpdates\safUcOGLqdWC Path: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2704 File: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (*WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, , , , , CREATE_SUSPENDED, , , , Process:2852:%WorkingDir%\GA BOR 08408 SHEET-LATVIA.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2704 Injected API: SetThreadContext		2704
Detection Detection Add File Detection Delete File Detection Call System API Call Process API	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%\System32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\System32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\System32\Tasks\Updates\safUcOGLqdWC Path: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2704 File: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, , , , CREATE_SUSPENDED, , , , Process:2852:%WorkingDir%\GA BOR 08408 SHEET-LATVIA.exe) Return: 1 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 Threat Characteristic: Resides in memory to evade detection		2704
Detection Add File Detection Delete File Detection Call System API Call Process API Detection	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%iSystem32ischtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%itmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%iSystem32iTasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%iSystem32iTasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%iSystem32iTasks\Updates\safUcOGLqdWC Path: %TEMP%itmp180.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2704 File: %TEMP%itmp180.tmp Type: VSDT_TEXT_HTML API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, , , , , CREATE_SUSPENDED, , , , Process:2852:%WorkingDir%\GA BOR 08408 SHEET-LATVIA.exe) Return: 1 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 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2704		2704
Detection Detection Add File Detection Delete File Detection Call System API Call Process API Detection	Threat Characteristic: Creates process in system directory Process ID: 2764 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\safUcOGLqdWC /XML %TEMP%\tmp180.tmp Threat Characteristic: Adds scheduled task to automatically run at startup Updates\safUcOGLqdWC /XML Path: %windir%\System32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\System32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\System32\Tasks\Updates\safUcOGLqdWC Path: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2704 File: %TEMP%\tmp180.tmp Type: VSDT_TEXT_HTML API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, , , , CREATE_SUSPENDED, , , , Process:2852:%WorkingDir%\GA BOR 08408 SHEET-LATVIA.exe) Return: 1 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 Threat Characteristic: Resides in memory to evade detection		2704

Detection	Throat Characteristic Creates areases		
Detection	Threat Characteristic: Creates process Process ID: 2704 Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe		
Call Virtual Memory API	Shell Command: API Name: WriteProcessMemory Args: (Process Name: 2852: % Working Dir % GABOR 08408 SHEET-LATVIA.exe, 400000, MZ., 1024, 18e508) Return: 1		2704
Detection	Threat Characteristic: Resides in memory to evade detection		2704
Delection	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, SUVWI\$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 I\$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%VGABOR 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%\Installi\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%InstallNost.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%InstallHost.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		
	API Name: GetDriveTypeW Args: (C:\) Return: 3	2704	2852
Call System API	74 Manie Steiner)powrage (C.) Notanie		

Call System API	API Name: GetDriveTypeW Args: (C\lambda) 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-ROM2.5+#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f	2704	2852
	2-00a0c91efb8b}\) Return: 5		
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0	2704	2852
	c91efb8b)\) Return: 3		
Call System API	API Name: GetDriveTypeW Args: (\"\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000006500000#{53f5630d-b6bf-11d0-94f2-00a0	2704	2852
	c91efb8b)\) Return: 3		
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%\In	2704	2852
Odii i Toocaa Ai T	stalliHost.exe) Return: 1	2104	2002
Detection	Threat Characteristic: Executes dropped file		
Scionicii	File: %APPDATA%InstalliHost.exe		
	Shell Command: %APPDATA%\Install\Host.exe "%APPDATA%\Install\Host.exe"		
Detection	Threat Characteristic: Creates process		
	Process ID: 2852		
	Image Path: %APPDATA%\InstalliHost.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
		2002	2092
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 ADI		2052	2002
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\dot*, 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\Nativelmages_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.		
	API Name: GetVersionExA Args: (779e1230) Return: 1	2852	2892
Call System API			2892
Call System API Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2852	
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information	2852	
	API Name: GetDriveTypeW Args: (C:\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2892	2852	
Call System API	Threat Characteristic: Executes commands or uses API to obtain system information	2852	
Call System API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2892	2852	2892
Call System API Detection Call System API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2892 Info: Obtains drive info from API result API Name: GetDriveTypeW Args: (C\(\chi\) Return: 3	2852	
Call System API Detection Call System API Call System API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2892 Info: Obtains drive info from API result API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3	2852 2852	2892
Call System API Detection Call System API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2892 Info: Obtains drive info from API result API Name: GetDriveTypeW Args: (C\(\chi\) Return: 3	2852	

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-ROM2.5+#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f} 2-00a0c91efb8b}\) Return: 5	2852	2892
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#000000000100000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\) Return: 3	2852	2892
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000006500000#{53f5630d-b6bf-11d0-94f2-00a0 c91efb8b}) \ Return: 3	2852	2892
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2852	2892
		2852	2892
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.exe, "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe, "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe\", , \	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		
2000au	Process ID: 2880 Image Path: %windir%\System32\WindowsPowerShell\u00e4In: 1.01powershell.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 "%	2852	2892
Sun 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	TEMP%\tmp1680.tmp",,,,,,%WorkingDir%,SW_HIDE, Process:1512:%windir%\System32\schtasks.exe) Return: 1	2002	2002
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%lsystem32\Tasks\Updates\safUcOGLqdWC Shell Command: %windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp1680.t mp"		
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\(\Lambda\) Return: 3	2892	2880
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2880		
0.110 / 45	Info: Obtains drive info from API result	0000	2000
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 API Name: GetDriveTypeW Args: (C:\) Return: 3	2892 2892	2880 2880
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2892	2880
Call System API Call System API	API Name: GetDriveTypeW Args: (C:\() Return: 3 API Name: GetDriveTypeW Args: (C:\() Return: 3	2892 2892	2880 2880
Call System API Call System API Call System API	API Name: GetDriveTypeW Args: (C:\() \) Return: 3 API Name: GetDriveTypeW Args: (C:\() \) Return: 3 API Name: GetDriveTypeW Args: (C:\() \) Return: 3	2892 2892 2892	2880 2880 2880
Call System API Call System API Call System API Call System API	API Name: GetDriveTypeW Args: (C\(\alpha\)) Return: 3	2892 2892 2892 2892	2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (C\(\alpha\)) Return: 3	2892 2892 2892 2892 2892	2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3	2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880
Call System API Write Registry Key	API Name: GetDriveTypeW Args: (CA) Return: 3	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880
Call System API Write Registry Key	API Name: GetDriveTypeW Args: (CA) Return: 3	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (C\1) Return: 3 API Name: GetDriveTypeW Args: ((\1) Return: 3 API Name: GetDriveTypeW Args: ((\1) Return: 3 API Name: GetDriveTypeW Args: ((\1) Return: 3 API Name: GetDriveTypeW Args: ((\1) Return: 3 API Name: GetDriveTypeW Args: ((\1) Return: 3 API Name: GetDriveTypeW Args: ((\1) Return: 3 API Name: GetDriveTypeW Args: ((\1) Return: 3 API Name: GetDriveTypeW Args: ((\1) Return: 3 API Name: GetDriveTypeW Args: ((\1) Return: 3	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: ((\(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: ((\(\text{\alpha}\) Return: 3 API Name: GetDriveTypeW Args: ((\(\text{\alpha}\) Return: 5 API Name: GetDriveTypeW Args: ((\(\text{\alpha}\) RAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#000000000000000000000000000000000000	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: (C \(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: ((\(\text{\chi}\) Return: 3 API Name: GetDriveTypeW Args: ((\(\text{\chi}\) RETURN AGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#000000000000000000000000000000000000	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 2	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3 API Name: GetDriveTypeW Args: (C.\) Return: 2 API Name: GetDriveTypeW Args: (C.\) Return: 2 API Name: GetDriveTypeW Args: (C.\) Return: 2 API Name: GetDriveTypeW Args: (C.\) Return: 2 API Name: GetDriveTypeW Args: (C.\) Return: 2 API Name: GetDriveTypeW Args: (C.\) Return: 2 API Name: GetDriveTypeW Args: (C.\) Return: 2 API Name: GetDriveTypeW Args: (C.\) Return: 2 API Name: GetDriveTypeW Args: (C.\) Return: 2	2892 2892 2892 2892 2892 2892 2892 2892	2880 2880 2880 2880 2880 2880 2880 2880

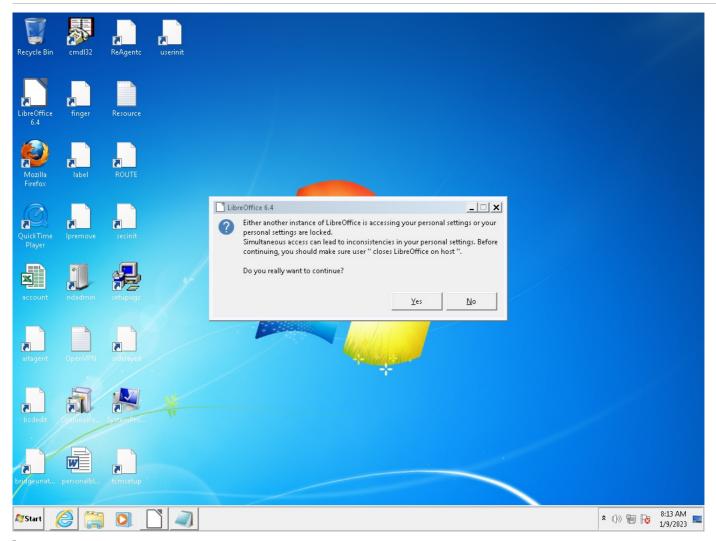
Call System API	API Name: GetDriveTypeW Args: (%windir%\) Return: 3	2892	2880
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms) Return: 1	2892	2880
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-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%IMicrosoft.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%IMicrosoft\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%Itmp1680.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\\$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\\$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		

Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2892 Target Process ID: 3044 Target Image: XAPPDATA%\Install\Host.exe		
Call Virtual Memory API	Injected Content: 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 Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 2	2892 2892	2880
Call System API		2892	2880
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2 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 Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 2	2704 2704	2740 2740
Detection	Threat Characteristic: Creates process in Application Data folder Process ID: 3044	2704	2140
	Image Path: %APPDATA%InstalfiHost.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 Detection	API Name: SleepEx Args: (INFINITE, 0) Return: 0 Threat Characteristic: Calls sleep function for an extended period	2892	2880
Social	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	2222	2011
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 API Name: socket Args: (204, 212, 193, 30, 230, 7324, 16.) Poturn: 0	2892	3044
Call Network API	API Name: connect Args: (204, 212.193.30.230:7324, 16) Return: 0	2892	3044
Detection Call Network API	Threat Characteristic: Establishes uncommon connection 212.193.30.230:7324 API Name: send Args: (204, A, 69, 0) Return: 69	2892	3044
Detection	Threat Characteristic: Connects to remote URL or IP address	2002	3044
	Content: A Content of the Content of		

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 Naturals ADI	ADI Namos socii Azon / 204 - 4 0 \ Deburo 2	3803	2044
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		2892	3044
	API Name: socket Args: (2, 1, 6) Return: 204		
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
	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
			3044
Call Network API		2802	
Call Network API Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69	2892	
Call Network API Call Network API Call System API	API Name: bnsQueryExW Args: (204, A, 69, 0) Return: 69 API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) Return: 0	2892	3044
Call Network API Call Network API	API Name: send Args: (204, A, 69, 0) Return: 69		
Call Network API Call Network API Call System API	API Name: bnsQueryExW Args: (204, A, 69, 0) Return: 69 API Name: DnsQueryExW Args: (212.193.30.230, 1, 50000000) 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	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B85
MD5	D41D8CD98F00B204E9800998ECF8427E
TLSH	-
Cimo	0 h- 4-(-)

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	F4F52BE1186C93ED5C7C927D9E59439BFAD548C995DA9203AC690BDC921D2E B4
MD5	C7C86B69E8A0E5534FBA8F1036FB5C7C
TLSH	-

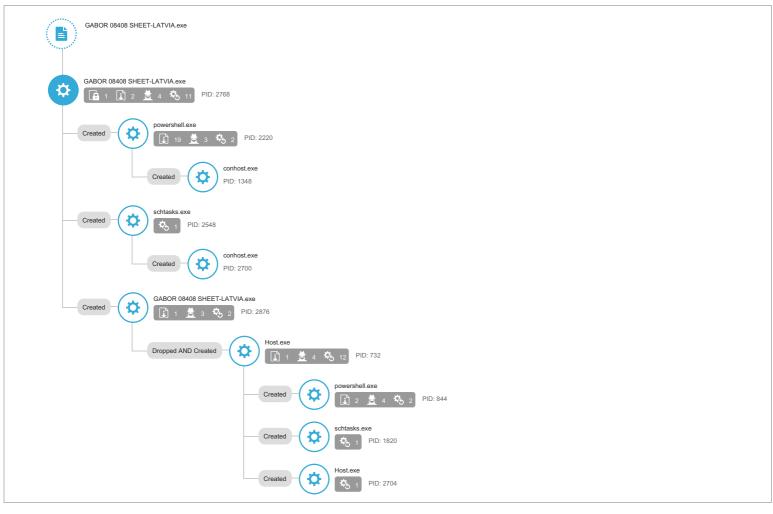
Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

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

GABOR 08408 SHEET-LATVIA.exe
MSIL Portable executable
2798A02A2A853DC16CABF2A062BC4E3069A6F0EA
F521274E6C6A1EBACEA6C13874170458C75199B5E61C3768B7F2DCFAC80975C 2
E5498B027F13F7BBB436E3356A6DA87D
-
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 <a> ☑

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

 $\ensuremath{\mathbb{G}}$ ATT&CKTM is a trademark of The MITRE Corporation.

▼ 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-Mg eference -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%\tmp2.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%\tmp2: .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%\tmp6" mp"
Executes dropped file	•	File: %TEMP%tmp68.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%tmp6 mp"
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%\ii024mgn.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-43f3-9482-8b624c919c 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-b020-4c0c624886 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-f2a3b9c76d 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-00214ee39c 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-6e09659cefa 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-0c42dcc922 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-cda4d36c17 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-b9247e73685c3 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-51375818d94 1 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%Intsv4n4f.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%ltmp68.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\\$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\\$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%\Instali\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.t mp"
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-MpPref erence -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-MpPref erence -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe"

▼ Rootkit, cloaking (1)

	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/MFEwTzBNMEswSTAJB gUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh% 2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7i90 VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk		GABOR 08408 SHEET-LATVIA.exe
http://ocsp.digicert.com/MFEwTzBNMEswSTAJB gUrDgMCGgUABBTBL0V27RVZ7LBduom%2Fn YB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7O rUETfACEA%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/upda te/v3/static/trustedr/en/disallowedcertstl.cab?dc4 e4acb3ff04861	Computers / Internet	No risk	-	GABOR 08408 SHEET-LATVIA.exe
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/pinrulesstl.cab?d0b176d4e 164f786	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
Hostexe	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	2798A02A2A853DC16CABF2A062BC4E3069 A6F0EA
safUcOGLqdWC.exe	Low	TROJ_GEN.R002C0DA723	Drops probable malware	-	742400	2798A02A2A853DC16CABF2A062BC4E3069 A6F0EA
t3apxthe.bwx.ps1	No risk	-	-	-	1	356A192B7913B04C54574D18C28D46E6395 428AB
lcyax2su.2xq.ps1	No risk	-	-	-	1	356A192B7913B04C54574D18C28D46E6395 428AB
d93f411851d7c929.customDestin ations-ms~RF10d97.TMP	No risk	-	-	-	6213	CD8E627A4194B369C62A4BF8790F12D5CA 0D941C
d93f411851d7c929.customDestin ations-ms	No risk	-	-	-	6213	7432F1A24F3AAC5CEEC6B5E6AB5D25A162 00C319
ZOUPON20X6SY3WN6Q4X2.tem	No risk	-	-	-	6213	7432F1A24F3AAC5CEEC6B5E6AB5D25A162 00C319
d93f411851d7c929.customDestin ations-ms	No risk	-	-	-	6213	B0C2D49DC29F674C57B63CE2ADB514FD5 DA095B4
Q8YXUTYZEX73JR63ILW7.temp	No risk	-	-	-	6213	B0C2D49DC29F674C57B63CE2ADB514FD5 DA095B4
d93f411851d7c929.customDestin ations-ms~RF129ab.TMP	No risk	-	-	-	6213	B0C2D49DC29F674C57B63CE2ADB514FD5 DA095B4

▼ Suspicious Objects

Туре	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: FindFirstFileEx/W 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	
0.11.57	Info: Obtains file or directory info from API result	0700
Call Filesystem API	API Name: FindNextFileW Args: (116adb8, eff164) Return: 1	2768 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
		2768
Call System API Call System API	API Name: GetVersionExA Args: (6e259cf0) Return: 1 API Name: System.Convert::FromBase64String Args: (14sIAAAAAAAEAO29B2AcSZYJJi9tynt/SvVK1+B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVm	2768
Call System AFT	VdZhZAzO2dvPfee++999577733ujudTif33/8/XGZkAWz2zkra) Return: 1F8B08000000000	2700
Detection	Threat Characteristic: Detected as obfuscated script File: GABOR 08408 SHEET-LATVIA.exe SHA1: 2798A02A2A853DC16CABF2A062BC4E3069A6F0EA	
Call System API		2769
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: System.Convert::FromBase64String Args: (VHJhbnNhY3Rpb25hbEIP) Return: 5472616E73616374	2768 2768
•	API Name: System.ConvertFrombasee4sting Ags. (VASIbilitin) 15 Return: 9472016273010374 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 15720808, 88) Return: 0	2768
Call System API		
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 15720764, 22) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 15720744, 18) Return: 0	2768
Call System API	API Name: System:Runtime.interopServices.marsnai::Copy Args: (89504E470D0ATA0A, 0, 15720744, 16) Return: 0	2768
L THE STREETON A MI	API News Contact Posting Internal Contact Marshall Contact Con	0700
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.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 105287480, 508002) Return: 0 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	2768 2768
Call System API Call System API Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 105287480, 508002) Return: 0 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: AdjustTokenPrivileges Args: (4b8, 0, , 0, , 8c8ebbc) Return: 1	2768
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 105287480, 508002) Return: 0 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	2768 2768
Call System API Call System API Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 105287480, 508002) Return: 0 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: AdjustTokenPrivileges Args: (4b8, 0, , 0, , 8c8ebbc) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2768	2768 2768
Call System API Call System API Call System API Detection	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 105287480, 508002) Return: 0 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: AdjustTokenPrivileges Args: (4b8, 0, , 0, , 8c8ebbc) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2768 Info: Obtains system level privileges	2768 2768 2768
Call System API Call System API Call System API Detection Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 105287480, 508002) Return: 0 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: AdjustTokenPrivileges Args: (4b8, 0, , 0, , 8c8ebbc) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2768 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period	2768 2768 2768
Call System API Call System API Call System API Detection Call System API Detection	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 105287480, 508002) Return: 0 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: AdjustTokenPrivileges Args: (4b8, 0, , 0, , 8c8ebbc) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2768 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 2768 slept for long or infinite time. Path: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Drops executable during installation Dropping Process ID: 2768 File: %APPDATA%\safUcOGLqdWC.exe	2768 2768 2768 2768
Call System API Call System API Call System API Detection Call System API Detection Add File	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 105287480, 508002) Return: 0 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: AdjustTokenPrivileges Args: (4b8, 0, , 0, , 8c8ebbc) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2768 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 2768 slept for long or infinite time. Path: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Drops executable during installation Dropping Process ID: 2768	2768 2768 2768 2768
Call System API Call System API Call System API Detection Call System API Detection Add File Detection	API Name: System.Renfection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: AdjustTokenPrivileges Args: (4D5A9000) Return: 0 API Name: AdjustTokenPrivileges Args: (4D5A9000) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2768 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 2768 slept for long or infinite time. Path: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Drops executable during installation Dropping Process ID: 2768 File: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Creates multiple copies of a file	2768 2768 2768 2768
Call System API Call System API Call System API Detection Call System API Detection Add File Detection Detection	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 105287480, 508002) Return: 0 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: AdjustTokenPrivileges Args: (4b8, 0, , 0, , 8c8ebbc) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2768 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 2768 slept for long or infinite time. Path: %APPDATA%/safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Drops executable during installation Dropping Process ID: 2768 File: %APPDATA%/safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Creates multiple copies of a file %APPDATA%/safUcOGLqdWC.exe Type: VSDT_EXE_MSIL	2768 2768 2768 2768
Call System API Call System API Call System API Detection Call System API Detection Add File Detection Detection	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 105287480, 508002) Return: 0 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: AdjustTokenPrivileges Args: (4b8, 0, , 0, , 8c8ebbc) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2768 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 2768 slept for long or infinite time. Path: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Drops executable during installation Dropping Process ID: 2768 File: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Creates multiple copies of a file %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Creates multiple copies of a file %APPDATA%\safUcOGLqdWC.exe Threat Characteristic: Copies self File is copied from %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe to %APPDATA%\safUcOGLqdWC.exe	2768 2768 2768 2768 2768
Call System API Call System API Call System API Detection Call System API Detection Add File Detection Detection Write File	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 105287480, 508002) Return: 0 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: AdjustTokenPrivileges Args: (4b8, 0, , 0, , 8c8ebbc) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2768 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 2768 slept for long or infinite time. Path: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Drops executable during installation Dropping Process ID: 2768 File: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Creates multiple copies of a file %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Copies self File is copied from %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe to %APPDATA%\safUcOGLqdWC.exe Path: %APPDATA%\safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems	2768 2768 2768 2768 2768
Call System API Call System API Call System API Detection Call System API Detection Add File Detection Detection Detection Detection Detection	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 105287480, 508002) Return: 0 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: AdjustTokenPrivileges Args: (4b8, 0, , 0, , 8c8ebbc) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2768 Indo: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 2768 slept for long or infinite time. Path: %APPDATA%isafUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Drops executable during installation Dropping Process ID: 2768 File: %APPDATA%isafUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Creates multiple copies of a file %APPDATA%isafUcOGLqdWC.exe Threat Characteristic: Copies self File is copied from %WorkingDir%iGABOR 08408 SHEET-LATVIA.exe to %APPDATA%isafUcOGLqdWC.exe Path: %APPDATA%isafUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%isafUcOGLqdWC.exe API Name: CopyFileExW Args: (%WorkingDir%iGABOR 08408 SHEET-LATVIA.exe, %APPDATA%isafUcOGLqdWC.exe, 0, 0, 0, 1) Return: 1 Threat Characteristic: Hides file to evade detection	2768 2768 2768 2768 2768
Call System API Call System API Call System API Call System API Detection Call System API Detection Add File Detection Detection Write File Detection Call Filesystem API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 105287480, 508002) Return: 0 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: AdjustTokenPrivileges Args: (4b8, 0, , 0, , 8c8ebbc) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2768 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 2768 slept for long or infinite time. Path: %APPDATA%safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Drops executable during installation Dropping Process ID: 2768 File: %APPDATA%safUcOGLqdWC.exe Type: VSDT_EXE_MSIL Threat Characteristic: Creates multiple copies of a file %APPDATA%safUcOGLqdWC.exe Threat Characteristic: Copies self File is copied from %WorkingDir%iGABOR 08408 SHEET-LATVIA.exe to %APPDATA%safUcOGLqdWC.exe Path: %APPDATA%safUcOGLqdWC.exe Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%safUcOGLqdWC.exe API Name: CopyFileExW Args: (%WorkingDir%iGABOR 08408 SHEET-LATVIA.exe, %APPDATA%safUcOGLqdWC.exe, 0, 0, 0, 1) Return: 1	2768 2768 2768 2768 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%lSysWOW64\propsys.dll) Return: 1		2768
Call System API			2768
	API Name: PathFileExistsW Args: (%windir%\Sys\WO\W64\propsys.dll) Return: 1		
Call System API	API Name: GelDriveTypeW Args: (\"\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\) 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)#00000000100000#(53f5630d-b6bf-11d0-94f2-00a		2768
Call System API	0c91efb8b}\) Return: 3 API Name: GetDriveTypeW Args: (\"\7\IDE#CdRomTEAC_CD-ROM		2768
Gail Gystom At 1	4f2-00a0c91efb8b)\) Return: 5		
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: GetDrive Lypew Args: (C.1) Return: 3 API Name: CreateProcessW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.exe, "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe"		2768
Call Process API	APT Name: Creater-rocessiv Args: ("wwindim's/systems/swindows-rowersneinv1.uppowersnein.exe, "wwindim's/systems/swindows-rowersneinv1.uppowe		2708
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-MpPref		
	erence -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 "%		2768
	TEMP%ltmp68.tmp", , , , CREATE_SUSPENDED, , %WorkingDir%, SW_HIDE, Process:2548:%windir%\SysWOW64\schtasks.exe) Return: 1		2700
Detection	Threat Characteristic: Executes dropped file %TEMP%\tmp68.tmp*		
Detection	Threat Characteristic: Executes dropped file File: windin%lsystem32/TasksUpdates\safUcOGLqdWC Sholl Company! windin%lsystem32/TasksU		
Detection	Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp68.tmp" Threat Characteristic: Executes dropped file		
Detection	File: %TEMP%Itmp68.tmp Shell Command: %windin%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: \(\frac{\text{windir}\%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe\)"\(\text{windir}\%\System32\WindowsPowerShell\v1.0\powershell.exe\)" \(\text{Add-MpPreference}\) ence -ExclusionPath \(\frac{\text{%APPDATA}\%\safUcOGLqd\WC.exe\)"		
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		2768	2220
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3 Threat Characteristic: Everutes commands or uses API to obtain system information	2768	
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/.) Neturn: 3	2768	2220
our system ru i			
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768	2220
Call System API		2769	2220
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768	2220
		2768 2768 2768	2220 2220 2220

0.110 / 4.701	150 A 15 T WA (6) D	0700	0000
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%\Sys\WOW64\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)#00000001F500000#(53f5630d-b6bf-11d0-94f2-00a	2768	2220
	0c91efb8b}\) Return: 3		
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000000100000#(53f5630d-b6bf-11d0-94f2-00a 0c91ef8bb)\\) Return: 3	2768	2220
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM2.5+#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-9 4f2-00a0c91efb8b)\) 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%IMicrosoft\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%IMicrosoftlWindows\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) R eturn: 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\Q8YXUTYZEX73JR63lLW7.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: (wwindir%\Microsoft.NET\Framework\\\^, 0, 93e6ac, 0, 0, 0) Return: b6c920	2768	2220
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	2.00	LLLV
Detection	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: FindFirstFileEx/W 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
	* 1		
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\mscoriib*, 0, 93ee28, 0, 0, 0) Return: b6c820	2768	2220
Add File	Path: %windir%lsystem32\Tasks\Updates\safUcOGLqdWC Type: VSDT_UNKNOWN		2768
Detection	Threat Characteristic: Adds scheduled task to automatically run at startup		
Detection	%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
· · · · · · · · · · · · · · · · · · ·		2768	2220
Call System API	API Name: AdjustTokenPrivileges Args: (4f0, 0, , 0, , 93e224) Return: 1 Threat Characteristic: Escalates process privileges to eain a higher level of access	2100	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%\GA		2768
	BOR 08408 SHEET-LATVIA.exe) Return: 1		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2768		
	Injected API: SetThreadContext Target Process ID: 2876		
	Target Image Path: %WorkingDir%IGABOR 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 Process ID: 2876 Target Process ID: 2876		
5	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:		
	API Name: WriteProcessMemory Args: (Process Name:2876:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 400000, MZ., 1024, efe3e8) Return: 1		2768
Call Virtual Memory API	Throat Characteristics Besides in moment to curde detection		
Call Virtual Memory API 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		
Detection	Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: MZ.		
	Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: MZ. Threat Characteristic: Injects memory with dropped files		
Detection	Injecting Process ID: 2768 Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe Injected Content: MZ.		

Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2876:%WorkingDir%IGABOR 08408 SHEET-LATVIA.exe, 401000, SUVWI\$4, 212992, efe3e8		2768
Detection) Return: 1 Threat Characteristic: Resides in memory to evade detection		
Betedion	Injecting Process ID: 2768		
	Target Process ID: 2876 Target Image Path: %WorkingDir%\GABOR 08408 SHEET-LATVIA.exe		
	Injected Content: SUVW\\$4'.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2876:%WorkingDir%IGABOR 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%IGABOR 08408 SHEET-LATVIA.exe		
	Injected Content: .SC		
Call Virtual Memory API Detection	API Name: WriteProcessMemory Args: (Process Name:2876:%WorkingDir%/GABOR 08408 SHEET-LATVIA.exe, 44b000, , 512, efe3e8) Return: 1 Threat Characteristic: Resides in memory to evade detection		2768
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		
O-II Victori Marco	Type: VSDT_TEXT_HTML ANNIAN WAR December 1 Anni Anni Anni Anni Anni Anni Anni An		0700
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7e91e000 Process:2876:%WorkingDir%\GABOR 08408 SHEET-LATVIA.exe, 7e91e008, , 4, efe3e8) R eturn: 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	0700	2768
Call Filesystem API Call Thread API	API Name: FindFirstFileExW Args: (%windir%lassembly/Nativelmages_v4.0.30319_32\System.Xml\ft, 0, 93b0a8, 0, 0, 0) Return: ad6df0 API Name: NtResumeThread Args: (Process:2876,) Return: ?	2768	2220
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2876], ppid[2768) Return: 1		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lassemblyNativeImages _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, 9689	2768	2220
	420) Return: 544		
Detection	Threat Characteristic: Creates named pipe \l\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 Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2	2768 2768	2220
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2 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
			2220
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2768	
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2768	2220
Call System API Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2	2768 2768	2220
Call System API Call System API Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2	2768 2768 2768	2220 2220
Call System API Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 2	2768 2768	2220
Call System API Call System API Call System API Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2	2768 2768 2768 2768	2220 2220 2220
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 2	2768 2768 2768 2768 2768	2220 2220 2220 2220
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 2	2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 2 API Name: GetDriveTypeW Args: (WTEMP%t/3apxthe.bwx.ps1\) Return: 3	2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\\3apxthe.bwx.ps1\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3	2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 2 API Name: GetDriveTypeW Args: (*TEMP%\\\\)13apxthe.bwx.ps\\\) Return: 3 API Name: GetDriveTypeW Args: (\\\\\\)COCALAPPDATA\(\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222
Call System API Add File	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 2 API Name: GetDriveTypeW Args: (WTEMP%\\\\) Return: 3 API Name: GetDriveTypeW Args: (\(\text{MTEMP}\\\\\)\) Return: 3 API Name: GetDriveTypeW Args: (\(\text{MUSERPROFILE}\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 2 API Name: GetDriveTypeW Args: (*TEMP%\\\\)13apxthe.bwx.ps\\\) Return: 3 API Name: GetDriveTypeW Args: (\\\\\\)COCALAPPDATA\(\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222

Write File	Path: %TEMP%\l3apxthe.bwx.ps1 Type: VSDT_ASCII	2768	2220
Add File	Path: %TEMP%Intsv4n4f.cgi.psm1 Type: VSDT_ASCII	2768	2220
Write File	Path: %TEMP%intsv4n4f.cgi.psm1 Type: VSDT_ASCII	2768	2220
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%lt3apxthe.bwx.ps1) Return: 1	2768	2220
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\ntsv4n4f.cgi.psm1) Return: 1	2768	2220
		2,00	
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	Dath, 0/TEMP0/Morantic house, 4/Temp//ODT ACCU	0700	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%ti3apxthe.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%Intsv4n4f.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%InstalliHost.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%Instalf\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
		2100	2010
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%InstalliHost.exe		
Call System API	API Name: GetDriveTypeW Args: (C/\) Return: 3	2768	2876
•		2700	2070
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%\Sys\WOW64\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-11d0-94f2-00a 0c91efb8b}\) Return: 3	2768	2876
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000000000000000000000000000000	2768	2876
Call System API	API Name: GetDriveTypeW Args: (\\?IDE#CdRomTEAC_CD-ROM2.5+#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		2768	2876
	API Name: GetDriveTypeW Args: (F:\) Return: 2		
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%, , Proces s: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 Shell Command: %APPDATA\(\)\Install\Host.exe		
Detection	Threat Characteristic: Creates process Process ID: 2876		
Betedion	Image Path: %APPDATA%\Install\Host.exe		
Call System API	Image Path: %APPDATA%InstalliHost.exe Shell Command: "%APPDATA%InstalliHost.exe" API Name: GetDriveTypeW Args: (E:\) Return: 2	2768	2220

Section Sect				
Selection	Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2768	2220
Million				
All	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
An International An International Continue An International An	Call Filesystem API	API Name: FindNextFileW Args: (7d2bb78, b92ebb4) Return: 1	2768	2220
Part	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules*, 0, b92eba4, 0, 0, 0) Return: 7d2b938	2768	2220
And Engrowed Parl	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Property	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Perspective	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Part	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Control Cont	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Control Cont	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*. 0. b92eaf8. 0. 0. 0) Return: 7d2bb78	2768	2220
Control Standard				
APT September APT APT APT September APT September APT September APT APT September APT APT September APT				
Mathematical April 1998 A				
March England No.				
March Part				
Processing	Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2768	2220
Coliman	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Mary March	Delete Registry Key	'	2768	2220
March March March Part	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
AP Name Part Pa	Write Registry Key		2768	2220
May MEX_10.5.1. MIX	Call Filesystem API		2768	2220
Page	•			
No. No. Nagary No. No. New York Co. Local Science 1906 1907	······································			
Column C	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\CimCmdlets*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
AFT Name Performance And AFT Name Performance AF	Write Registry Key		2768	2220
Afficiency March Afficiency Afficien	Call Filesystem API		2768	2220
Properties AT An Internet Fortier EACM Args. (Swindfridingsherit2/amtosegowershelm (Bibloos) intelligent/bosenschart), 0.05/eacs, 0.0.1 (pleasm. 76.0) 229 2				
Part Parcy plant Program Prof. Part		2b938		
Dept	·	2b938		
Call Filosystem API	Call Filesystem API		2768	2220
Call Placystom API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Dism*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Fisophern APP	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	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Dism*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Cast Filesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DnsClient*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
API Name Froit F	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DnsClient*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Cast Fisterystem AP	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DnsClient*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
API Name: FindFirstFieEsW Age: (Neindri-Nogstein-32bin/dosepowershalls of 2000 delection (17 political paragraphs)			2768	
Call Filesystem API	•			
Call Filesystem API				
Call Fleeystem AP API Name: FindFirstFileEXW Aggs. (Wwindri\u00e4) (Septem API API Name: Fi				
Call Filesystem API				
Call Filesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Fleeystem API API Name: FindFirstFileExW Args: (%windir%laystem32windowspowershelltv 1.0Modulesi8CSIV: 0, 16/2eaac, 0, 0, 0) Return: 7d2bb78 278 2220 Call Fleeystem API API Name: FindFirstFileExW Args: (%windir%laystem32windowspowershelltv 1.0Modulesi8CSIV: 0, 16/2eaac, 0, 0, 0) Return: 7d2bb78 278 2220 Call Fleeystem API API Name: FindFirstFileExW Args: (%windir%laystem32windowspowershelltv 1.0Modulesi8EX: 0, 16/2eaac, 0, 0, 0) Return: 7d2bb78 2788 2220 Call Fleeystem API API Name: FindFirstFileExW Args: (%windir%laystem32windowspowershelltv 1.0Modulesi8EX: 0, 16/2eaac, 0, 0, 0) Return: 7d2bb78 2788 2220 Call Fleeystem API API Name: FindFirstFileExW Args: (%windir%laystem32windowspowershelltv 1.0Modulesi8Csv, 0, 16/2eaac, 0, 0, 0) Return: 7d2bb78 2788 2220 Call Fleeystem API API Name: FindFirstFileExW Args: (%windir%laystem32windowspowershelltv 1.0Modulesi8Csv, 0, 16/2eaac, 0, 0, 0) Return: 7d2bb78 2788 2220 Call Fleeystem API API Name: FindFirstFileExW Args: (%windir%laystem32windowspowershelltv 1.0ModulesiMcrosoft PowerShell Archiver, 0, b1/2eaac, 0, 0, 0) Return: 7d2bb78 2788 2220 Call Fleeystem API API Name: FindFirstFileExW Args: (%windir%laystem32windowspowershelliv 1.0ModulesiMicrosoft PowerShell Archiver, 0, b1/2eaac, 0, 0, 0) Return: 7d2b 2788 2220 Call Fleeystem API <td< td=""><td>Call Filesystem API</td><td>API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International\t^*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938</td><td>2768</td><td>2220</td></td<>	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International\t^*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%leystem32windowspowershelliv1.0Modules)BCSN*, 0, b62eas6, 0, 0, 0) Return: 7d2bb78 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%leystem32windowspowershelliv1.0Modules)BEX*, 0, b62easc, 0, 0, 0) Return: 7d2bb78 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%leystem32windowspowershelliv1.0Modules)BEX*, 0, b62easc, 0, 0, 0) Return: 7d2bb38 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%leystem32windowspowershelliv1.0Modules)BEX*, 0, b62easc, 0, 0, 0) Return: 7d2bb38 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%leystem32windowspowershelliv1.0Modules)Mcds*, 0, b62easc, 0, 0, 0) Return: 7d2bb38 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%leystem32windowspowershelliv1.0Modules)Mcrosoft.PowerShell.Archivel*, 0, b62easc, 0, 0, 0) Return: 7d2bb38 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%leystem32windowspowershelliv1.0Modules)Mcrosoft.PowerShell.Archivel*, 0, b62easc, 0, 0, 0) Return: 7d2bb38 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%leystem32windowspowershelliv1.0Modules)Mcrosoft.PowerShell.Archivel*, 0, b62easc, 0, 0, 0) Return: 7d2bb38 2768 2220 Call Filesystem AP	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	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelllv1.0\Modules\iSCSI*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	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: (%winds*\system32\windowspowershelltv1.0\Modules\USE**, 0, b92easc, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%winds*\system32\windowspowershelltv1.0\Modules\USE**, 0, b92easc, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%winds*\system32\windowspowershelltv1.0\Modules\Use\USe**, 0, b92easc, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%winds*\system32\windowspowershelltv1.0\Modules\Use\USe\\sin^*, 0, b92easc, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%winds*\system32\windowspowershelltv1.0\Modules\Use\User\user\undowspowershelltv1.0\Modules\User\undowspowershelltv1.0\modul	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\\SE*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78		
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershell/v1.0Modules\Microsoft, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershell/v1.0Modules\Mcds**, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershell/v1.0Modules\Mcds**, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershell/v1.0Modules\Microsoft.PowerShell.Archivel*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershell/v1.0Modules\Microsoft.PowerShell.Archivel*, 0, b92eaf8, 0, 0, 0) Return: 7d2b 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershell/v1.0Modules\Microsoft.PowerShell.Archivelen-USi*, 0, b92e8b4, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershell/v1.0Modules\Microsoft.PowerShell.Archivelen-USi*, 0, b92e8b4, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershell/v1.0Modules\Microsoft.PowerShell.Archivelen-USi*, 0, b92ea60, 0, 0, 0) Return: 7d2b938 2768				
Call Flesystem API API Name: FindFirstFileExW Args: (%windir%)system32windowspowershelliv1.0ModulesiMcrosoft. PowerShell Archive/sn. 0, b92eaac, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%)system32windowspowershelliv1.0ModulesiMcrosoft.PowerShell.Archive1*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%)system32windowspowershelliv1.0ModulesiMcrosoft.PowerShell.Archive1*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%)system32windowspowershelliv1.0ModulesiMicrosoft.PowerShell.Archive1*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%)system32windowspowershelliv1.0ModulesiMicrosoft.PowerShell.Archive1*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%)system32windowspowershelliv1.0ModulesiMicrosoft.PowerShell.Archive1*en-US1*, 0, b92e964, 0, 0, 0) Return: 7d2b93 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%)system32windowspowershelliv1.0ModulesiMicrosoft.PowerShell Archive1*n-US1*, 0, b92ea60, 0, 0, 0) Return: 7d2b93 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%)system32windowspowershelliv1.0ModulesiMicrosoft.PowerShell.Diagno				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%/system32\windowspowershelliv1.0\Modules\Mcdis\Mcdis\Novales\Mcdis\N				
Call Filesystem API API Name: FindFirstFileExW Args. (%windir%lsystem32\windowspowershelltv1.0!ModulesiMicrosoft.PowerShell.Archive1*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args. (%windir%lsystem32\windowspowershelltv1.0!ModulesiMicrosoft.PowerShell.Archive1*, 0, b92eaac, 0, 0, 0) Return: 7d2b 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args. (%windir%lsystem32\windowspowershelltv1.0!ModulesiMicrosoft.PowerShell.Archive1*, 0, b92eaac, 0, 0, 0) Return: 7d2b 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args. (%windir%lsystem32\windowspowershelltv1.0!ModulesiMicrosoft.PowerShell.Archive1en-USi*, 0, b92e9b4, 0, 0, 0) Return: 7d2b98 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args. (%windir%lsystem32\windowspowershelltv1.0!ModulesiMicrosoft.PowerShell.Archive1en-USi*, 0, b92ea00, 0, 0, 0) Return: 7d2b98 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args. (%windir%lsystem32\windowspowershelltv1.0!ModulesiMicrosoft.PowerShell.Archive1en-USi*, 0, b92ea00, 0, 0, 0) Return: 7d2b98 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args. (%windir%lsystem32\windowspowershelltv1.0!ModulesiMicrosoft.PowerShell.Diagnosticsi*, 0, b92eaac, 0, 0, 0) Return: 7d2b98 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args. (%windir%lsystem32\windowspowershelltv1.0!ModulesiMicrosof				
API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelltv1.0\Modules\Microsoft.PowerShell.Archive\t^*, 0, b92eaac, 0, 0, 0) Return: 7d2b 938 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelltv1.0\Modules\Microsoft.PowerShell.Archive\t^*, 0, b92eaac, 0, 0, 0) Return: 7d2b 938 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelltv1.0\Modules\Microsoft.PowerShell.Archive\ten-US\t^*, 0, b92eab4, 0, 0, 0) Return 7d2b6938 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelltv1.0\Modules\Microsoft.PowerShell.Archive\ten-US\t^*, 0, b92eab4, 0, 0, 0) Return 7d2b698 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelltv1.0\Modules\Microsoft.PowerShell.Archive\ten-US\t^*, 0, b92eab0, 0, 0, 0) Return 7d2b69 2768 2220 Call Filesystem API API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelltv1.0\Modules\Microsoft.PowerShell.Archive\t^*, 0, b92eab0, 0, 0, 0) Return: 7d2b69 38 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelltv1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, b92eab0, 0, 0, 0) Return: 7d2b69 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelltv1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, b92eaac, 0, 0, 0) Return: 7d2b69 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelltv1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, b92eaac, 0, 0, 0) Return: 7d2b69 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelltv1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, b92eaac, 0, 0, 0) Return: 7d2b69 2768 2220				
938 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\Microsoft.PowerShell.Archive\tau, 0, b92eaac, 0, 0, 0) Return: 7d2b 938 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\Microsoft.PowerShell.Archive\tau-US\tau, 0, b92e9b4, 0, 0, 0) Return 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\Microsoft.PowerShell.Archive\tau-US\tau, 0, b92eabd, 0, 0, 0) Return 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\Microsoft.PowerShell.Archive\tau-US\tau, 0, b92eabd, 0, 0, 0) Return 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\Microsoft.PowerShell.Archive\tau, 0, b92eabd, 0, 0, 0) Return: 7d2b9 38 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\Microsoft.PowerShell.Diagnostics\tau, 0, b92eaac, 0, 0, 0) Return: 7 d2b9 d2b938 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\Microsoft.PowerShell.Diagnostics\tau, 0, b92eaac, 0, 0, 0) Return: 7 d2b9 d2b938 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\Microsoft.PowerShell.Diagnostics\tau, 0, b92eaac, 0, 0, 0) Return: 7 d2b9 d2b938 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\Microsoft.PowerShell.Diagnostics\tau, 0, b92eaac, 0, 0, 0) Return: 7 d2b9 d2b938	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Kds*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938		2220
API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92e9b4, 0, 0, 0) Return 2768 2220 220 220 220 220 220 220 220 220 2	Call Filesystem API		2768	2220
2220 call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92ea9b4, 0, 0, 0) Return 7d2b938 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 2768 2220 call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92ea18, 0, 0, 0) Return: 7d2b9 2768 2220 call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92ea18, 0, 0, 0) Return: 7 2768 2220 call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7 2768 2220 call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7 2768 2220 call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92ea18, 0, 0, 0) Return: 7 2768 2220 call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92ea18, 0, 0, 0) Return: 7 2768 2220 call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92ea18, 0, 0, 0) Return: 7 2768 2220 call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92ea18, 0, 0, 0) Return: 7 2768 2220 call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92ea18, 0, 0, 0) Return: 7 2768 2220 call Filesystem API API Name: FindFir	Call Filesystem API		2768	2220
2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\n-US\n^*, 0, b92ea00, 0, 0, 0) Return: 7d2b9 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\n^*, 0, b92eaf8, 0, 0, 0) Return: 7d2b9 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\n^*, 0, b92eaac, 0, 0, 0) Return: 7 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\n^*, 0, b92eaac, 0, 0, 0) Return: 7 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\n^*, 0, b92eaac, 0, 0, 0) Return: 7 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\n^*, 0, b92eaf8, 0, 0, 0) Return: 7 2768 2220	Call Filesystem API		2768	2220
API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\ten-US*, 0, b92ea00, 0, 0, 0) Return: 7d2b93 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\tau^*, 0, b92eaf8, 0, 0, 0) Return: 7d2b9 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, b92eafc, 0, 0, 0) Return: 7 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, b92eaac, 0, 0, 0) Return: 7 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, b92eaac, 0, 0, 0) Return: 7 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, b92eaf6, 0, 0, 0) Return: 7 2768 2220	Call Filesystem API		2768	2220
API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\t^*, 0, b92eaf8, 0, 0, 0) Return: 7d2b9 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, b92eaac, 0, 0, 0) Return: 7 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, b92eaac, 0, 0, 0) Return: 7 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, b92eaf8, 0, 0, 0) Return: 7 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, b92eaf8, 0, 0, 0) Return: 7 2768 2220	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\t^*, 0, b92ea00, 0, 0, 0) Return	2768	2220
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaf8, 0, 0, 0) Return: 7 2768 2220	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92eaf8, 0, 0, 0) Return: 7d2b9	2768	2220
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7 d2b938 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaf8, 0, 0, 0) Return: 7 d2b938 2220 2768 2220	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7	2768	2220
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaf8, 0, 0, 0) Return: 7 d2b938 2768 2220	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7	2768	2220
	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaf8, 0, 0, 0) Return: 7	2768	2220
	Call Filesystem API		2768	2220
		Telumination of the second of		

Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host\v1^*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileEx\W 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\v1, 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\t^*, 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\t^*, 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: 7d 2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\v, 0, b92eaac, 0, 0, 0) Return: 7d	2768	2220
Call Filesystem API	2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e9b4, 0, 0, 0) Ret	2768	2220
Call Filesystem API	um: 7d2b938 API Namer: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e9b4, 0, 0, 0) Ret	2768	2220
Call Filesystem API	um: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92ea00, 0, 0, 0) Ret	2768	2220
Call Filesystem API	um: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\v0,0,b92eaf8,0,0,0) Return: 7d	2768	2220
Call Filesystem API	2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92eaac, 0, 0, 0) Return: 7d2b	2768	2220
Call Filesystem API	938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92eaac, 0, 0, 0) Return: 7d2b	2768	2220
Call Filesystem API	938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92eaf8, 0, 0, 0) Return: 7d2b	2768	2220
Call Filesystem API	938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\t^*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f	2768	2220
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershellIv1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92eaac, 0, 0, 0) Return: 7d2b93	2768	2220
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\tv1.0\tiModules\Microsoft.PowerShell.Utility*, 0, b92eaf8, 0, 0, 0) Return: 7d2b93	2768	2220
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\w1.0\lModules\Microsoft.WSMan.Management\v1.0\ b92eaac, 0, 0, 0) Return: 7d2	2768	2220
	bb78		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management\v*, 0, b92eaac, 0, 0, 0) Return: 7d2 b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management\v*, 0, b92eaf8, 0, 0, 0) Return: 7d2 b938	2768	2220
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\MsDtc*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExtW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\MsDtc*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileEx:W Args: (%windir%lsystem32\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%Installhost.exe		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetAdapten*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetAdapter\t^*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetAdapten*, 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: FindFirstFileEx/W Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetConnection*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetEventPacketCapture*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileEx/W 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: FindFirstFileEx/W Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetLbfo*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetNat*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileEx/W 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%lsystem32\windowspowershell\v1.0\Modules\NetQos*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\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
			732
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lassemblyNativeImages_v4.0.30319_32\imscorlib*, 0, 67f248, 0, 0, 0) Return: b77520 API Name: FindFirstFileExW Args: (%windir%lassemblyNativeImages_v4.0.30319_32\imscorlib*, 0, 67f248, 0, 0, 0) Return: b77520	2876 2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%)system32\windowspowershell\v1.0\Modules\NetSecurity*, 0, b92eaac, 0, 0, 0) Return: 7d2b938		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetSecurity*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768	2220
C-II Fil AB'	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSwitchTeam*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	ADI News First First First First Annual (0) winding ()		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSwitchTeam*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\n'1.0\lModules\NetSwitchTeam*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\n'1.0\lModules\NetSwitchTeam*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\n'1.0\lModules\NetTCPIP*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768 2768 2768	2220 2220 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%lassembly\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: 7d2b93 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d2bb7 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaf8, 0, 0, 0) Return: 7d2b93 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\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%lsystem32\windowspowershell\v1.0\Modules\PK\I*, 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\t^*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindNextFileW Args: (7d/2bb78, 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\t^*, 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: 7d2b	2768	2220
Call Filesystem API	938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b92eaac, 0, 0, 0) Return: 7d2b	2768	2220
	938		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b92eaf8, 0, 0, 0) Return: 7d2b 938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\PSDiagnostics*, 0, b92eaac, 0, 0, 0) Return: 7d2b9f8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\PSDiagnostics\t^*, 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%lsystem32\windowspowershelllv1.0\Modules\PSScheduledJob*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\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
			LLLO
			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 Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768 2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732	2768	
Call Filesystem API Call Filesystem API Call System API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access	2768 2768	2220
Call Filesystem API Call Filesystem API Call System API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732	2768 2768	2220
Call Filesystem API Call Filesystem API Call System API Detection	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges	2768 2768 2876	2220 732
Call Filesystem API Call Filesystem API Call System API Detection Call System API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period	2768 2768 2876	2220 732
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaaa, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time.	2768 2768 2876 2876	732 732
Call Filesystem API Call System API Call System API Detection Call System API Detection Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768 2768 2876 2876 2876	2220 732 732 2220
Call Filesystem API Call System API Call System API Detection Call System API Detection Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b918	2768 2768 2876 2876 2876	2220 732 732 2220 2220
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b918 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938	2768 2768 2876 2876 2876 2768 2768 2768	2220 732 732 2220 2220 2220
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768 2768 2876 2876 2876 2768 2768 2768	2220 732 732 2220 2220 2220 2220
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Stor3tLS*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Stor3tLS*, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768 2768 2876 2876 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Stor3t\system30, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Stor3t\system30, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Stor3t\system30, 0, 0) Return: 7d2b978	2768 2768 2876 2876 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b92eaf8, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b92eaf8, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\wi	2768 2876 2876 2876 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\Storage\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage	2768 2876 2876 2876 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b92eaac, 0, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirst	2768 2876 2876 2876 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir\system32\windowspowershell\v1.0\Modules\Storage*, 0, b92eaf8, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (\mathematical \math	2768 2876 2876 2876 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 2220 2220 2220 2220 2220 2220
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%\system32\windowspowershelliv1.0\Modules\SecureBoott*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (wwindir%\system32\windowspowershelliv1.0\Modules\SecureBoott*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, 1, 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (wwindir%\system32\windowspowershelliv1.0\Modules\Storage\forage\forage, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (wwindir%\system32\windowspowershelliv1.0\Modules\Storage\forage\forage, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (wwindir%\system32\windowspowershelliv1.0\Modules\Storage\forage\forage, 0, b92eaf8, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (wwindir%\system32\windowspowershelliv1.0\Modules\Storage\forage\forage, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (wwindir%\system32\windowspowershelliv1.0\Modules\Storage\forage\forage, 0, b92eaac, 0, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (wwindir%\system32\windowspowershelliv1.0\Modules\Storage\forage\forage, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (wwindir%\system32\windowspowershelliv1.0\Modules\Storage\forage\forage, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (wwindir%\system32\windowspowershelliv1.0\Modules\Storage\forage\forage, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (wwindir%\system32\windowspowershelliv1.0\Modules\Storage\forage\forage, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (wwindir%\system32\windowspowershelliv1.0\Modules\Storage\forage\forage, 0, 0, 0) Return: 7d2b938 API Name: FindFi	2768 2876 2876 2876 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelliv1.0\Modules\SecureBoot 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelliv1.0\Modules\SecureBoot 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, 0, 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Storage 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Storage 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Storage 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage 0, b92eaf8, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\Storage 0, b92eaf8, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\Storage 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\Storage 0, b92eaac, 0, 0, 0) Return: 7d2bb938 API Name: FindFirstFileExW Args: (%windir%\system32\windowsp	2768 2876 2876 2876 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SieepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaf8, 0, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershel	2768 2876 2876 2876 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelliv1.0\Modules\SecureBoot 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelliv1.0\Modules\Storage 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Storage 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Storage 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Storage 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage 0, b92eaf8, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\Storage 0, b92eaf8, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\Storage 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\Storage 0, b92eaac, 0, 0, 0) Return: 7d2bb938 API Name: FindFirstFileExW Args: (%windir%\system32\windowspo	2768 2876 2876 2876 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SieepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaf8, 0, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0\Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32\windowspowershel	2768 2876 2876 2876 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22
Call Filesystem API Call System API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, 0, 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 sleept for long or infinite time. API Name: FindFirstFileExW Args: (\(\) \(\	2768 2876 2876 2876 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API	API Name: FindFirstFileExW Ags: (%windir%isystem32\windowspowershelliv 1.0\Modules\SecureBoot\footnote{N}, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Ags: (36, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Into: Oblatins system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 sleep to for long or infinite time. API Name: FindFirstFileExW Args: (\(\) \(2768 2876 2876 2876 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22
Call Filesystem API Call System API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API Call System API Detection	API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0\Modules\SecureBoot\footnote{N}, 0, b92ealac, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3fc, 0, , 0, , 7e0f13c) Return: 1 Threat Characteristis: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristis: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFielExW Args: (\windir%lsystem32\windowspowershelliv1.0\Modules\Storage\footnote{N}, 0, b92ealac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFielExW Args: (\windir%lsystem32\windowspowershelliv1.0\Modules\Storage\footnote{N}, 0, b92ealac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFielExW Args: (\windir%lsystem32\windowspowershelliv1.0\Modules\Storage\footnote{N}, 0, b92ealac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFielExW Args: (\windir%lsystem32\windowspowershelliv1.0\Wodules\Storage\footnote{N}, 0, b92ealac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFielExW Args: (\windir%lsystem32\windowspowershelliv1.0\Wodules\Storage\footnote{N}, 0, b92ealac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFielExW Args: (\windir%lsystem32\windowspowershelliv1.0\Wodules\TLS\footnote{N}, 0, b92ealac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFielExW Args: (\windir%lsystem32\windowspowershelliv1.0\Wodules\TLS\footnote{N}, 0, b92ealac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFielExW Args: (\windir%lsystem32\windowspowershelliv1.0\Wodules\TLS\footnote{N}, 0, b92ealac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFielExW Args: (\windir%lsystem32\windowspowershelliv1.0\Wodules\TroubleshootingPack\footnote{N}, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFielExW Args: (\windir%lsystem32\windowspowershelliv1.0\Wodules\TroubleshootingPack\footnote{N}, 0, b92eaac, 0, 0, 0) Return: 7d2bb938 API Name: FindFirstFielExW Args: (\windir%lsystem32\window	2768 2876 2876 2876 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22
Call Filesystem API Call Filesystem API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API Call System API	API Name: FindFirstFieExW Args: (%windir%system32windowspowershellv1.0Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFieExW Args: (%windir%system32windowspowershellv1.0Modules\SecureBoot*, 0, b92eaf8, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3/c, 0, 0, ., 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFieExW Args: (%windir%system32windowspowershellv1.0Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFieExW Args: (%windir%system32windowspowershellv1.0Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFieExW Args: (%windir%system32windowspowershellv1.0Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFieExW Args: (%windir%system32windowspowershellv1.0Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFieExW Args: (%windir%system32windowspowershellv1.0Modules\Tto*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFieExW Args: (%windir%system32windowspowershellv1.0Modules\Tto*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFieExW Args: (%windir%system32windowspowershellv1.0Modules\TroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFieExW Args: (%windir%system32windowspowershellv1.0Modules\TroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFieExW Args: (%windir%system32windowspowershellv1.0Modules\TroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFieExW Args: (%windir%system32windowspowershellv1.0Modules\TroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFieExW Args: (%windir%system32windowspowershellv1.0Modules\TroubleshootingPack*, 0,	2768 2876 2876 2876 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22
Call Filesystem API Call System API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API Call System API	API Name: FindFirstFileExW Args: (%windir%system32windowspowershellv1.0Modules\SecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: AdjustTokenPrivileges Args: (3c, 0, 0, ., 7e0f13c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process 10; 732 Info: Obtains system level privileges API Name: SleepEx Args: (2000, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%system32windowspowershellv1.0Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32windowspowershellv1.0Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32windowspowershellv1.0Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32windowspowershellv1.0Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32windowspowershellv1.0Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32windowspowershellv1.0Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%system32windowspowershellv1.0Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%system32windowspowershellv1.0Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%system32windowspowershellv1.0Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78 API Name: FindFirstFileExW Args: (%windir%system32windowspowershellv1.0Modules\Storage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32windowspowershellv1.0Modules\StorabehootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%system32windowspowershellv1.0Modules\StorabehootingPack*, 0, b92eaac, 0, 0, 0) Retu	2768 2876 2876 2876 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22
Call Filesystem API Call System API Call System API Detection Call System API Detection Call System API Detection Call Filesystem API Call System API	API Name: FindFirstFileExW Args: (%windir%isystem32windowspowershellv1.0ModulestSecureBoot*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: AglustTokenPrivileges Args: (36c, 0, 0, 7e0f13e) Return: 1 Tiveat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 732 Intro Oblains system level privileges API Name: AglustTokenPrivileges Args: (30c, 0, 1) Return: 0 Threat Characteristic: Calls sleep function for an extended period Process 732 slept for long or infinite time. API Name: FindFirstFileExW Args: (%windir%isystem32/windowspowershellv1.0ModulestStorage*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%isystem32/windowspowershellv1.0ModulestStorage*, 0, b92eaac, 0, 0, 0) Return: 7d2b983 API Name: FindFirstFileExW Args: (%windir%isystem32/windowspowershellv1.0ModulestStorage*, 0, b92eaac, 0, 0, 0) Return: 7d2b983 API Name: FindFirstFileExW Args: (%windir%isystem32/windowspowershellv1.0ModulestTus*, 0, b92eaac, 0, 0, 0) Return: 7d2b983 API Name: FindFirstFileExW Args: (%windir%isystem32/windowspowershellv1.0ModulestTus*, 0, b92eaac, 0, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%isystem32/windowspowershellv1.0ModulestTus*, 0, b92eaac, 0, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%isystem32/windowspowershellv1.0ModulestTus*, 0, b92eaac, 0, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%isystem32/windowspowershellv1.0ModulestTroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2b978 API Name: FindFirstFileExW Args: (%windir%isystem32/windowspowershellv1.0ModulestTroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%isystem32/windowspowershellv1.0ModulestTroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%isystem32/windowspowershellv1.0ModulestTroubleshootingPack*, 0, b92eaac, 0, 0, 0) Return: 7d2b938 API Name: FindFirstFileExW Args: (%windir%isystem32/windowspowershellv1.0Module	2768 2876 2876 2876 2768 2768 2768 2768	2220 732 732 2220 2220 2220 2220 2220 22

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-11d0-94f2-00a 0c91efb8b}\) 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: (*/ 3848200) Return: 7d2b9f 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsDeveloperLicense*, 0, b92eaac, 0, 0, 0) Return: 7d2b93 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsDeveloperLicense\t^*, 0, b92eaf8, 0, 0, 0) Return: 7d2b93 8	2768	2220
Call System API		2876	732
Call System API	API Name: GelDriveTypeW Args: (\\?\DE#CdRomTEAC_CD-ROM	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		2876	732
	API Name: GetDriveTypeA Args: (C.\) Return: 3 API Name: GetEnregroundWindow Args: () Return: 100r2	2876	
Call System API	API Name: GetForegroundWindow Args: () Return: 100c2	2010	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\powe	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%lsystem32\windowspowershell\v1.0\Modules\WindowsErrorReporting*, 0, b92eaac, 0, 0, 0) Return: 7d2bb78	2768	2220
Call Filesystem API		2768	2220
	API Name: FindFirstFileExW Args: (%windir%)system32\windowspowershell\v1.0\Modules\WindowsErrorReporting\v1, 0, b92eaac, 0, 0, 0) Return: 7d2b938		
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\t, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86) %\WindowsPowerShell\Modules\PackageManagement\t, 0, b92eaac, 0, 0, 0) Return: 7d2b938	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0\tau, 0, b92e9b4, 0, 0, 0) Return: 7d2b9 38	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0\founds, 0, b92e9b4, 0, 0, 0) Return: 7d2b9 38	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0\tau, 0, b92ea00, 0, 0, 0) Return: 7d2bb 78	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\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		2876	732
•	API Name: GetForegroundWindow Args: () Return: 100c2	2070	
Call System API	API Name: GetForegroundWindow Args: () Return: 100c2 API Name: GetDriveTypeW Args: (C:\(\alpha\)) Return: 3	2876	732
			732 732
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%	2876	
Call System API Call Process API	API Name: GetDriveTypeW Args: (C:\) Return: 3 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 Threat Characteristic: Executes dropped file	2876	
Call System API Call Process API Detection	API Name: GetDriveTypeW Args: (C:\() Return: 3 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 Threat Characteristic: Executes dropped file %TEMP%\tmp2313.tmp* 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.t	2876	
Call System API Call Process API Detection Detection	API Name: GetDriveTypeW Args: (C\(\) Return: 3 API Name: CreateProcessW Args: (\(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(2876	
Call System API Call Process API Detection Detection Detection	API Name: GetDriveTypeW Args: (C\(\) Return: 3 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 Threat Characteristic: Executes dropped file \%TEMP\%\tmp2313.tmp" Threat Characteristic: Executes dropped file \%Tie: \%TEMP\%\tmp2313.tmp Threat Characteristic: Executes dropped file \%Tie: \%windir\%\System32\schtasks.exe "\%windir\%\System32\schtasks.exe" / Create /TN "Updates\safUcOGLqdWC" / XML "\%TEMP\%\tmp2313.tmp Threat Characteristic: Executes dropped file \%Tie: \%windir\%\System32\schtasks.exe "\%windir\%\System32\schtasks.exe" / Create /TN "Updates\safUcOGLqdWC" / XML "\%TEMP\%\tmp2313.tmp"	2876	732
Call System API Call Process API Detection Detection Detection Call System API	API Name: GetDriveTypeW Args: (C\() Return: 3 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 Threat Characteristic: Executes dropped file %TEMP%\tmp2313.tmp" 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 Threat Characteristic: Executes dropped file File: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp 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" API Name: GetForegroundWindow Args: () Return: 100c2	2876	732
Call System API Call Process API Detection Detection Call System API Call Thread API	API Name: GetDriveTypeW Args: (C\() Return: 3 API Name: GetDriveTypeW 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 Threat Characteristic: Executes dropped file %TEMP%\tmp2313.tmp" Threat Characteristic: Executes dropped file File: %TEMP%\tmp2313.tmp Threat Characteristic: Executes dropped file File: %TEMP%\tmp2313.tmp Threat Characteristic: Executes dropped file File: %TeMP%\tmp2313.tmp Threat Characteristic: Executes dropped file File: %Windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp" 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" API Name: GetForegroundWindow Args: () Return: 100c2 API Name: NtResumeThread Args: (Process:1820,) Return: ?	2876 2876 2876 2876	732 732 732
Call System API Call Process API Detection Detection Detection Call System API Call Thread API Call System API Call System API	API Name: GetDriveTypeW Args: (C\() Return: 3 API Name: GetDriveTypeW Args: (\(\) Wwindir\(\) System32\(\) Schtasks.exe, "\(\) "wwindir\(\) System32\(\) Schtasks.exe" / Create /TN "Updates\(\) afucure: 1 Threat Characteristic: Executes dropped file %TEMP\(\) "Impa313.tmp" Threat Characteristic: Executes dropped file #File: \(\) "EEWP\(\) "Impa313.tmp" Threat Characteristic: Executes dropped file #File: \(\) "EEWP\(\) "Impa313.tmp" Threat Characteristic: Executes dropped file #File: \(\) "EEWP\(\) "Impa313.tmp Threat Characteristic: Executes dropped file #File: \(\) "EWP\(\) "Impa313.tmp Threat Characteristic: Executes dropped file #File: \(\) "Windir\(\) "System32\(\) "Schtasks.exe" "\(\) "Windir\(\) "System32\(\) "Schtasks.exe" / Create /TN "Updates\(\) safUCOGLqdWC" /XML "\(\) "TEMP\(\) \(\) Temp2313.tmp' Threat Characteristic: Executes dropped file #File: \(\) "windir\(\) "System32\(\) "Schtasks.exe" "\(\) "windir\(\) "System32\(\) "Schtasks.exe" "\(\) "Updates\(\) safUcOGLqdWC" /XML "\(\) "TEMP\(\) \(\) Temp2313.tmp' API Name: GetForegroundWindow Args: () Return: 100c2 API Name: NiResumeThread Args: (\(\) Process:1820,) Return: 2 API Name: evtchann.SendEvent Args: (\(\) ProgramFiles(x86)\(\) "WindowsPowerShellModules\(\) Pestern'*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2876 2876 2876 2876 2876	732 732 732 732
Call System API Call Process API Detection Detection Detection Call System API Call Thread API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: GetDriveTypeW Args: (C\() Return: 3 API Name: GetDriveTypeW 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 Threat Characteristic: Executes dropped file %TEMP%\tmp2313.tmp" Threat Characteristic: Executes dropped file File: %TEMP%\tmp2313.tmp Threat Characteristic: Executes dropped file File: %TEMP%\tmp2313.tmp Threat Characteristic: Executes dropped file File: %TeMP%\tmp2313.tmp Threat Characteristic: Executes dropped file File: windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp" Threat Characteristic: Executes dropped file File: \(\text{windir}\%\System32\schtasks.exe \(\text{"windir}\%\System32\schtasks.exe" \) /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp" API Name: GetForegroundWindow Args: () Return: 100c2 API Name: evtchann.SendEvent Args: (\(\text{Process:1820},) \) Return: ? API Name: FindFirstFileExW Args: (\(\text{"ProgramFiles(x86)}\\ \WindowsPowerShell\Modules\Pester*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (\(\text{"ProgramFiles(x86)}\\ \WindowsPowerShell\Modules\Pester*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2876 2876 2876 2876 2876 2768	732 732 732 732 2220 2220
Call Process API Detection Detection Detection Call System API Call Thread API Call Filesystem API	API Name: GetDriveTypeW Args: (C:\() Return: 3 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 Threat Characteristic: Executes dropped file %TEMP%\tmp2313.tmp" 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" Threat Characteristic: Executes dropped file File: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp" Threat Characteristic: Executes dropped file File: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp" API Name: GetForegroundWindow Args: () Return: 100c2 API Name: NitResumeThread Args: (Process:1820,) Return: ? API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2876 2876 2876 2876 2876 2768 2768	732 732 732 732 2220 2220
Call System API Call Process API Detection Detection Detection Call System API Call Thread API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: GetDriveTypeW Args: (C\() Return: 3 API Name: GetDriveTypeW 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 Threat Characteristic: Executes dropped file %TEMP%\tmp2313.tmp" Threat Characteristic: Executes dropped file File: %TEMP%\tmp2313.tmp Threat Characteristic: Executes dropped file File: %TEMP%\tmp2313.tmp Threat Characteristic: Executes dropped file File: %TeMP%\tmp2313.tmp Threat Characteristic: Executes dropped file File: windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp" Threat Characteristic: Executes dropped file File: \(\text{windir}\%\System32\schtasks.exe \(\text{"windir}\%\System32\schtasks.exe" \) /Create /TN "Updates\safUcOGLqdWC" /XML "%TEMP%\tmp2313.tmp" API Name: GetForegroundWindow Args: () Return: 100c2 API Name: evtchann.SendEvent Args: (\(\text{Process:1820},) \) Return: ? API Name: FindFirstFileExW Args: (\(\text{"ProgramFiles(x86)}\\ \WindowsPowerShell\Modules\Pester*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (\(\text{"ProgramFiles(x86)}\\ \WindowsPowerShell\Modules\Pester*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2876 2876 2876 2876 2876 2768	732 732 732 732 2220 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\PowerShellGett*, 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	$API\ Name: FindFirstFileExW\ Args: (\ \%ProgramFiles (x86)\% \ Windows PowerShellModules \ PowerShellGet \ 1,0,b92eaac,0,0,0)\ Return: 7d39be0$	2768	2220
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	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: FindFirstFileExtW 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%lsystem32\WindowsPowerShelllv1.0\Modules\AppLocken*, 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\t^*, 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%lsystem32\WindowsPowerShelllv1.0\Modules\BranchCache*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExtW 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
	• • • • • • • • • • • • • • • • • • • •		2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b92eaac, 0, 0, 0) Return: 7 d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b92eaac, 0, 0, 0) Return: 7	2768	2220
	d39be0		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b92eaf8, 0, 0, 0) Return: 7d	2768	2220
	39be0		
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: FindFirstFileExtW 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%lsystem32\WindowsPowerShelllv1.0\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\v1, 0, b92eaac, 0, 0, 0) Return: 7d39be	2768	2220
Call Filesystem AFT	7. Traine. Fillul ilsu ileExtrags. (//willuli //isystemisztviilluws/ owersitemi/ 1.0/iiiuuules/Event racingmanagement , 0, 052eaac, 0, 0, 0) retuini. 705566	2700	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\EventTracingManagement\t^*, 0, b92eaac, 0, 0, 0) Return: 7d39be	2768	2220
	0		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b92eaf8, 0, 0, 0) Return: 7d39be	2768	2220
	0		
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	$API\ Name: FindFirstFileExW\ Args: (\ windir\%lsystem 32 \ Windows Power Shell \ v1.0 \ Modules \ International \ v, 0, b92 eaac, 0, 0, 0)\ Return: 7d39be0$	2768	2220
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\%lsystem 32 \ Windows Power Shell \ 1.0 \ Modules \ International \ 1,0,b92eaf 8,0,0,0)\ Return: 7d39be0$	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\iSCS*, 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\\SE*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\\SE*, 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%lsystem32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\t^*, 0, b92eaac, 0, 0, 0) Return: 7d3	2768	2220
	9be0		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\t^*, 0, b92eaac, 0, 0, 0) Return: 7d3 9be0	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
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92e9b4, 0, 0, 0) Return 3 (200b.0)	2768	2220
Call Filesystem API	n: 7d39be0		
Call Filesystem API Call Filesystem API	n: /d390e0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92ea00, 0, 0, 0) Retur n: 7d39be0	2768	2220
	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b92ea00, 0, 0, 0) Returns the control of the c	2768 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 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92ea68, 0, 0, 0) Return: 7d39		
Call Filesystem API 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 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive**, 0, b92eaf8, 0, 0, 0) Return: 7d39be0 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.Archive\en-US*, 0, b92ea80, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92ea86, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92ea68, 0, 0, 0) Return: 7d39be0	2768 2768 2768 2768	2220 2220 2220 2220
Call Filesystem API 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 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92ea68, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92ea68, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768 2768 2768 2768 2768	2220 2220 2220 2220 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 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92ea68, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92ea6, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b92ea6, 0, 0, 0) Return: 7d39be0	2768 2768 2768 2768	2220 2220 2220 2220

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\v, 0, b92eaac, 0, 0, 0) Return	2768	2220
Call Filesystem API	: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\v0, 0, b92eaac, 0, 0, 0) Return	2768	2220
	: 7d39be0		
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: 7 d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell\.ODataUtils*, 0, b92eaac, 0, 0, 0) Return: 7	2768	2220
Call Filesystem API	d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e9b4, 0, 0, 0) R	2768	2220
our resystem Ar i	etum: 7d39be0	2700	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e9b4, 0, 0, 0) R eturn: 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) R eturn: 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: 7	2768	2220
0.85% 4.48%	d39be0	0700	0000
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92eaac, 0, 0, 0) Return: 7d3 9be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92eaac, 0, 0, 0) Return: 7d3 9be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\(^*, 0, b92eaf8, 0, 0, 0) Return: 7d3	2768	2220
Call Filesystem API	9be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility 0, b92eaac, 0, 0, 0) Return: 7d39b	2768	2220
	e0		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92eaac, 0, 0, 0) Return: 7d39b e0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92eaf8, 0, 0, 0) Return: 7d39b e0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\Microsoft.WSMan.Management\(^*, 0, b92eaac, 0, 0, 0 \) Return: 7d	2768	2220
Call Filesystem API	39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Managemenft*, 0, b92eaac, 0, 0, 0) Return: 7d	2768	2220
Call Filesystem AFT	39be0	2700	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Managemenft*, 0, b92eaf8, 0, 0, 0) Return: 7d 39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\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\NetAdapten*, 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%lsystem32\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, b92eaf\(8, 0, 0, 0 \) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0lModules\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%lsystem32\WindowsPowerShelllv1.0\Modules\NetNatt*, 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\t^*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity\t^*, 0, b92eaf8, 0, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API		2768	2220
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b92eaac, 0, 0, 0) Return: 7d39be0		
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			2220
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API 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 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetWorkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39b	2768 2768	2220 2220
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768 2768 2768	2220 2220 2220
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaaf, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39b	2768 2768 2768 2768	2220 2220 2220 2220
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768 2768 2768 2768 2768	2220 2220 2220 2220 2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetWorkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetworkConnectivityStatus*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0	2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be e0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be e0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be e0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be e0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d39be e1 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d39be e1 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d39be e1 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d39be e1 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d39be e1	2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetWorkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768 2768 2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\PnpDevice\t^*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\PnpDevice\t^*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768	2220
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\PripDevice*, 0, b92eaf8, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b92eaac, 0, 0, 0) Return: 7d39be0	2768 2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32/WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b92eaac, 0, 0, 0) Return: 7d39be0 API Name: FindFirstFileExW Args: (%windir%lsystem32/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-MpPrefer ence -ExclusionPath "%APPDATA%\safUcOGLqdWC.exe"		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-42 6c-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_771a0ed5-7c01-4b ee-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 T ype: 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-4b2 4-83f7-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%IMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49fc-8c8a-57e7c5b6bc48 T ype: 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: DeletteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49 fc-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-48 66-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-a8e1-40 8e-ad40-b9247e73685c) Return: 1	2768	2220
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	732	844
Call Filesystem API	API Name: DeletteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0f570e6e-bc60-4e d9-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:\(\alpha\)) 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: \SDT_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\(\Lambda\) 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/L) 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%IMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15952f2e-49c7-4619-8d6e-eb9ab3d779cd T ype: 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-49c7-46 19-8d6e-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%MicrosoftWindows\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-42 20-8151-cda4d36c1796) Return: 1	2768	2220
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4ecb-aeed-0c42dcc9225b T ype: 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%MicrosoftWindows\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-4e cb-aeed-0o42dcc9225b) 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#\olume#\(ee5e3854\)-dde6-11eb-9bdd-806e6\(f6e6963\)\#000000001F500000\(#\)\f53f5630d-b6bf-11d0-94f2-00a 0c91efb8b\)\) Return: 3	732	844
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6/6e6963)#0000000000000000000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\)	732	844
Call System API	API Name: GelDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	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%IMicrosoft(Windows)PowerShell/CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefac Ty	2768	2220
	pe: VSDT_COM_DOS		
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 Process ID: 2220 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefac Type: \SDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404 e-b04b-6e09659cefac) Return: 1	2768	2220
Delete File	Path: %TEMP%ltmp2313.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 T ype: 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: \SDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-48 37-bf5e-00214ee39c04) Return: 1	2768	2220
Call Process API	37-0fbe-00214ee39c04) Return: 1 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 Injecting 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 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-49	2768	2220
	5a-bde2-f2a3b9c76d25) Return: 1		
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6afe8b90, -1, a4e454, a4e450, 0) Return: 0	732	844
Delete File	Path: %LOCALAPPDATA%MicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-495a-bde2-f2a3b9c76d25 T ype: 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\\$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\\$4\\$4\\$5.		
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	2010	702
	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%\Instalf\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	Injected Address: 0x0 API Name: SetThreadContext Args: (Process Name:2704:%APPDATA%\Install\Host.exe) Return: 1	2876	732
Call Thread API Call System API	·	2876 732	732 844
	API Name: SetThreadContext Args: (Process Name:2704:%APPDATA%\Install\Host.exe) Return: 1		
Call System API	API Name: SetThreadContext Args: (Process Name: 2704: %APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3 API Name: NtResumeThread Args: (Process: 2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42	732	844
Call System API Call Thread API Call Filesystem API	API Name: SetThreadContext Args: (Process Name: 2704: %APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3 API Name: NtResumeThread Args: (Process: 2704,) Return: ?	732 2876 2768	844 732
Call System API Call Thread API	API Name: SetThreadContext Args: (Process Name: 2704: %APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir\\System32\Windows\PowerShell\v1.0\)) Return: 3 API Name: NtResumeThread Args: (Process: 2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1	732 2876	844 732 2220
Call System API Call Thread API Call Filesystem API Call System API	API Name: SetThreadContext Args: (Process Name: 2704: %APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShellv1.0\)) Return: 3 API Name: NtResumeThread Args: (Process: 2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1	732 2876 2768 2876	844 732 2220 732
Call System API Call Thread API Call Filesystem API Call System API	API Name: SetThreadContext Args: (Process Name:2704:%APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir\System32\WindowsPowerShell\v1.0\)) Return: 3 API Name: NtResumeThread Args: (Process:2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type : VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection	732 2876 2768 2876	844 732 2220 732
Call System API Call Filesystem API Call System API Call System API Delete File	API Name: SetThreadContext Args: (Process Name: 2704: %APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir\System32\WindowsPowerShell\v1.0\)) Return: 3 API Name: NtResumeThread Args: (Process: 2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type: VSDT_COM_DOS 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	732 2876 2768 2876	844 732 2220 732
Call System API Call Filesystem API Call Filesystem API Call System API Delete File Detection	API Name: SetThreadContext Args: (Process Name: 2704: %APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\), Return: 3 API Name: NtResumeThread Args: (Process: 2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type : VSDT_COM_DOS 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	732 2876 2768 2876 2876 2768	844 732 2220 732 2220
Call System API Call Filesystem API Call Filesystem API Call System API Delete File Detection Call System API	API Name: SetThreadContext Args: (Process Name: 2704: %APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3 API Name: NtResumeThread Args: (Process: 2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid(2704), ppid(732) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type : VSDT_COM_DOS 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 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3	732 2876 2768 2876 2876 2768	844 732 2220 732 2220
Call System API Call Filesystem API Call Filesystem API Call System API Delete File Detection Call System API Add File	API Name: SetThreadContext Args: (Process Name: 2704: %APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir\System32\WindowsPowerShell\v1.0\) Return: 3 API Name: NtResumeThread Args: (Process: 2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type : VSDT_COM_DOS 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 API Name: GetDriveTypeW Args: (%windir\System32\Windows\PowerShell\v1.0\) Return: 3 Path: %APPDATA%\Microsoft\Windows\Recent\CostomDestinations\ZOUPON20X6SY3\WN6Q4X2.temp Type: VSDT_COM_DOS	732 2876 2768 2876 2876 2768	844 732 2220 732 2220
Call System API Call Thread API Call Filesystem API Call System API Delete File Detection Call System API	API Name: SetThreadContext Args: (Process Name: 2704: %APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3 API Name: NtResumeThread Args: (Process: 2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid(2704), ppid(732) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type : VSDT_COM_DOS 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 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3	732 2876 2768 2876 2768 732	844 732 2220 732 2220
Call System API Call Filesystem API Call Filesystem API Call System API Delete File Detection Call System API Add File Call System API	API Name: SetThreadContext Args: (Process Name: 2704: %APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3 API Name: NtResumeThread Args: (Process: 2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988e-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type : VSDT_COM_DOS 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 API Name: GetDriveTypeW Args: (%windir%\System32\Windows\PowerShell\v1.0\) Return: 3 Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\Recent\Recent\CustomDestinations\Recent\CustomDestinations\Recent\Recent\Recent\Recent\Recent\Recent\Recent\Recent\Recent\Recent\Recent\Recent\Recent\Recent\Recent\Recont\Recent\Recent\Recent\Recent\Recent\Recent\Recent\Recent\Rece	732 2876 2768 2876 2768 732 732 732	844 732 2220 732 2220 844 844 844
Call System API Call Filesystem API Call Filesystem API Call System API Delete File Detection Call System API Add File Call System API Write File	API Name: SetThreadContext Args: (Process Name: 2704: %APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3 API Name: NtResumeThread Args: (Process: 2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type : VSDT_COM_DOS 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 API Name: GetDriveTypeW Args: (%windir%\System32\Windows\PowerShell\v1.0\) Return: 3 Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS	732 2876 2768 2876 2768 2768 732 732 732 732	844 732 2220 732 2220 844 844 844 844
Call System API Call Filesystem API Call Filesystem API Call System API Delete File Detection Call System API Add File Call System API Write File Add File	API Name: SetThreadContext Args: (Process Name: 2704: %APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3 API Name: NtResumeThread Args: (Process: 2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988e-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type : VSDT_COM_DOS 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 API Name: GetDriveTypeW Args: (%windir\\System32\Windows\PowerShell\v1.0\) Return: 3 Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\ZOUPON\Z0X6SY3W\N6Q4X2.temp Type: VSDT_COM_DOS API Name: PathFileExists\W Args: (%APPDATA\Microsoft\Windows\Recent\CustomDestinations\ZOUPON\Z0X6SY3W\N6Q4X2.temp Type: VSDT_COM_DOS Path: %APPDATA\Microsoft\Windows\Recent\CustomDestinations\ZOUPON\Z0X6SY3W\N6Q4X2.temp Type: VSDT_COM_DOS Path: %APPDATA\Microsoft\Windows\Recent\CustomDestinations\ZOUPON\Z0X6SY3W\N6Q4X2.temp Type: VSDT_COM_DOS Path: %APPDATA\Microsoft\Windows\Recent\CustomDestinations\ZOUPON\Z0X6SY3W\N6Q4X2.temp Type: VSDT_COM_DOS Path: %APPDATA\Microsoft\Windows\Recent\CustomDestinations\ZOUPON\Z0X6SY3W\N6Q4X2.temp Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms-RF129ab.TMP) R	732 2876 2768 2876 2768 2768 732 732 732 732 732 732	844 732 2220 732 2220 844 844 844 844
Call System API Call Filesystem API Call Filesystem API Call System API Call System API Delete File Detection Call System API Add File Call System API Write File Add File Call Filesystem API Call Filesystem API	API Name: SetThreadContext Args: (Process Name: 2704: %APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3 API Name: NtResumeThread Args: (Process: 2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988e-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type : VSDT_COM_DOS 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 API Name: GetDriveTypeW Args: (%windir\\System32\Windows\PowerShell\v1.0\) Return: 3 Path: %APPDATA\Microsoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%APPDATA\Microsoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS Path: %APPDATA\Microsoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS Path: %APPDATA\Microsoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS Path: %APPDATA\Microsoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS Path: %APPDATA\Microsoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF129ab.TMP Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF129ab.TMP Type: VSDT_COM_DOS	732 2876 2768 2876 2768 732 732 732 732 732 732 732 732	844 732 2220 732 2220 844 844 844 844 844 844
Call System API Call Filesystem API Call Filesystem API Call System API Call System API Delete File Detection Call System API Add File Call System API Write File Add File Call Filesystem API Add File Add File Add File Add File Call Filesystem API	API Name: SetThreadContext Args: (Process Name:2704:%APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) \ Return: 3 API Name: NiResumeThread Args: (Process:2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type : VSDT_COM_DOS 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 API Name: GetDriveTypeW Args: (%windir%\System32\Windows\PowerShell\v1.0\) \ Return: 3 Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\zouPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\zouPoN2	732 2876 2768 2876 2768 2768 732 732 732 732 732 732 732 732	844 732 2220 732 2220 844 844 844 844 844 844 844
Call System API Call Filesystem API Call Filesystem API Call System API Call System API Delete File Detection Call System API Add File Call System API Write File Add File Call Filesystem API Add File Call Filesystem API	API Name: SetThreadContext Args: (Process Name:2704:%APPDATA%IInstalliHost.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShellV1.0\) Return: 3 API Name: NiResumeThread Args: (Process:2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%IMicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1 Path: %LOCALAPPDATA%IMicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type : VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%IMicrosoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type: VSDT_COM_DOS API Name: GetDriveTypeW Args: (%windir%\System32\Windows\PowerShell\V1.0\) Return: 3 Path: %APPDATA%IMicrosoft\Windows\Recent\CustomDestinations\tZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%APPDATA%IMicrosoft\Windows\Recent\CustomDestinations\tZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%APPDATA%IMicrosoft\Windows\Recent\CustomDestinations\td93f411851d7c929.customDestinations-ms) Return: 1 Path: %APPDATA%IMicrosoft\Windows\Recent\CustomDestinations\td93f411851d7c929.customDestinations-ms-RF129ab.TMP Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%IMicrosoft\Windows\Recent\CustomDestinations\td93f411851d7c929.customDestinations-ms-RF129ab.TMP) R eturn: 1 Path: %APPDATA%IMicrosoft\Windows\Recent\CustomDestinations\td93f411851d7c929.customDestinations-ms-RF129ab.TMP) R eturn: 1 Path: %APPDATA%IMicrosoft\Windows\Recent\CustomDestinations\td93f411851d7c929.customDestinations-ms-RF129ab.TMP) R eturn: 1	732 2876 2768 2876 2768 2876 2768 732 732 732 732 732 732 732 732 732 732	844 732 2220 732 2220 844 844 844 844 844 844 844 84
Call System API Call Filesystem API Call Filesystem API Call System API Call System API Delete File Detection Call System API Add File Call System API Write File Add File Call Filesystem API Add File Add File Add File Add File Call Filesystem API	API Name: SetThreadContext Args: (Process Name:2704:%APPDATA%\Install\Host.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) \ Return: 3 API Name: NiResumeThread Args: (Process:2704,) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type : VSDT_COM_DOS 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 API Name: GetDriveTypeW Args: (%windir%\System32\Windows\PowerShell\v1.0\) \ Return: 3 Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\zouPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\zouPoN2	732 2876 2768 2876 2768 2768 732 732 732 732 732 732 732 732	844 732 2220 732 2220 844 844 844 844 844 844 844
Call System API Call Filesystem API Call Filesystem API Call System API Call System API Delete File Detection Call System API Add File Call System API Write File Add File Call Filesystem API	API Name: SetThreadContext Args: (Process Name: 2704:%APPDATA%IInstalliHost.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%iSystem32\WindowsPowerShell\V1.0\) Return: 3 API Name: NtResumeThread Args: (Process:2704,) Return: 7 API Name: DeleteFileW Args: (%LOCALAPPDATA%IMicrosoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1 Path: %LOCALAPPDATA%iMicrosoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type : VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%iMicrosoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type: VSDT_COM_DOS API Name: GetDriveTypeW Args: (%windir%iSystem32\Windows\PowerShell\V1.0\) Return: 3 Path: %APPDATA%iMicrosoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%APPDATA%iMicrosoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoft\Windows\Recent\CustomDestinations\ZOUPON20X6SY3WN6Q4X2.temp Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%windir\South\Xindows\Recent\Custo	732 2876 2768 2876 2768 2876 2768 732 732 732 732 732 732 732 732 732 732	844 732 2220 732 2220 844 844 844 844 844 844 844 84
Call System API Call Filesystem API Call Filesystem API Call System API Call System API Delete File Detection Call System API Add File Call System API Write File Add File Call Filesystem API	API Name: SetThreadContext Args: (Process Name: 2704:%APPDATA%linstalliHost.exe) Return: 1 API Name: GetDriveTypeW Args: (%windir%iSystem32!WindowsPowerShelliV1.0\)) Return: 3 API Name: NtResumeThread Args: (Process:2704.) Return: ? API Name: DeleteFileW Args: (%LOCALAPPDATA%iMicrosoftiWindows\PowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[2704], ppid[732) Return: 1 Path: %LOCALAPPDATA%iMicrosoftiWindows\PowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2220 File: %LOCALAPPDATA%iMicrosoftiWindows\PowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type: VSDT_COM_DOS API Name: GetDriveTypeW Args: (%windir%iSystem32!WindowsPowerShelliV1.0\)) Return: 3 Path: %APPDATA%iMicrosoftiWindows\RecentiCustomDestinations\ZOUPON2XGSY3WN6Q4X2.temp Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%APPDATA%iMicrosoftWindows\RecentiCustomDestinations\d934f11851d7c929.customDestinations-ms - RF129ab.TMP Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoftiWindows\RecentiCustomDestinations\d934f11851d7c929.customDestinations-ms - RF129ab.TMP Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%APPDATA%iMicrosoftWindows\RecentiCustomDestinations\d934f11851d7c929.customDestinations-ms - RF129ab.TMP Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%iMicrosoftWindows\RecentiCustomDestinations\d934f11851d7c929.customDestinations-ms - RF129ab.TMP Type: VSDT_COM_DOS API Name: PathFileExistW Args: (%APPDATA%iMicrosoftWindows\RecentiCustomDestinations\d934f11851d7c929.customDestinations-ms - RF129ab.TMP Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%windir%iMicrosoftNEThFramework\V^*, 0, a4e69c, 0, 0, 0) Return: e	732 2876 2768 2876 2768 2876 2768 732 732 732 732 732 732 732 732 732 732	844 732 2220 732 2220 844 844 844 844 844 844 844 84

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		
211 5	Info: Obtains system level privileges	0700	0000
Delete File	Path: %LOCALAPPDATA%MicrosoftWindows\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-1d73-4	2768	2220
	2ce-b020-4c0c62488e1d) Return: 1		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66d89b97-f9aa-43f3-9482-8b624c919cb7 T	2768	2220
	ype: VSDT_COM_DOS		
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-43 f3-9482-8b624c919cb7) Return: 1	2768	2220
Call Filesystem ADI	*	2769	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		
2000.01	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\t, 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: acb5a	2768	2220
	08		
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement\1.0.0.0*, 0, b92e344, 0, 0, 0) Return: acb5a 08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b92e390, 0, 0, 0) Return: acb5b	2768	2220
	08		
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)%WindowsPowerShellfModules\PowerShellGet\tau, 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		2768	2220
Call I llesystem AFT	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b92e534, 0, 0, 0) Return: acb5a08	2/00	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules*, 0, b92e534, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\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	
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768 2768	2220
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e488, 0, 0, 0) Return: acb5a8	2768 2768 2768	2220 2220
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e48c, 0, 0, 0) Return: acb5c88 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768 2768 2768 2768	2220 2220 2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768 2768 2768 2768 2768	2220 2220 2220 2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Wodules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Wodules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Wodules\AppLocker*, 0, b92e488, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Wodules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Wodules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Wodules\Appx*, 0, b92e488, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Wodules\Appx*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\AppLocker*, 0, b92e488, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Appx*, 0, b92e488, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Appx*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e48c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e48c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e48c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e48c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e48c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e48c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e48c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e48c, 0, 0, 0) Return: acb5a08	2768 2768 2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e48e, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, b92e48e, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, b92e48e, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, b92e48e, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e48e, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e48e, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e48e, 0, 0, 0) Return: acb5a08	2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e48a, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e48a, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e48a, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e48a, 0, 0, 0) Return: acb5a08	2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e48c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e48c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e48c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e48c, 0, 0, 0) Return: acb5a08	2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Nam	2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%wind	2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b92e43c, 0, 0, 0) Return: acb5a08 API Nam	2768 2768 2768 2768 2768 2768 2768 2768	2220 2220 2220 2220 2220 2220 2220 222

Call Filosystom API	ADI Namo: EindEiretEilaEvW Aras: (%uindir%\nustam20\MindousPauerPauerShallud 0\Madulas\DiractAccossCliontComponents)* 0, b02x489, 0, 0, 0, \ Datura: ac	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b92e488, 0, 0, 0) Return: ac b5c48	2/08	2220
Call Filesystem API	API Name: FindFirstFileExtW 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: FindFirstFileExtW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient\t^*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b92e43c, 0, 0, 0) Return: acb5c4 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a0 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b92e488, 0, 0, 0) Return: acb5a0 8	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\t^*, 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: FindFirstFileEx/W Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SCS*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS(\t^*, 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%lsystem32\WindowsPowerShelllv1.0\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
· · · · · · · · · · · · · · · · · · ·	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds\\^, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API			
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: acb5 a88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92e43c, 0, 0, 0) Return: acb5 a08	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: acb5 a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\\^, 0, b92e43c, 0, 0, 0) Return:	2768	2220
Call Filesystem API	acb5c48 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\footnote{1}, 0, b92e43c, 0, 0, 0) Return:	2768	2220
Call Filesystem API	acb5a08 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 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\v1.0, b92e43c, 0, 0, 0) Return: acb5a0 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92e43c, 0, 0, 0) Return: acb5a0 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92e488, 0, 0, 0) Return: acb5a0 8	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: a cb5c88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b92e43c, 0, 0, 0) Return: a cb5c88	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) R eturn: 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) R eturn: 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) R eturn: 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: a cb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92e43c, 0, 0, 0) Return: acb 5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92e43c, 0, 0, 0) Return: acb 5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92e488, 0, 0, 0) Return: acb 5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\t^*, 0, b92e43c, 0, 0, 0) Return: acb5c 48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92e43c, 0, 0, 0) Return: acb5a 08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\t^*, 0, b92e488, 0, 0, 0) Return: acb5c 48	2768	2220

Communication Communicatio				
Professionaries Profession	Call Filesystem API		2768	2220
An Service Institutional or any Treatment of Service	Call Filesystem API		2768	2220
March March Telephon An important production and production of the product of the production o	·	b5c88		
Anthony of the Principal Continues of the Prin	Call Filesystem API		2768	2220
All Service Artificial of the process of the proc	Call Filesystem API		2768	2220
A Principal Pr				
Michael Michael Enther Section 1985 200				
March Marc	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b92e488, 0, 0, 0) Return: acb5c48		2220
Milliame Professional of State Professional of Sta	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Miles Mile	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\%lsystem 32 \ windows PowerShell \ v1.0 \ word ules \ NetAdapter \ v1,0,092e43c,0,0,0)\ Return: acb5a08$	2768	2220
Comment	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Description And All Notes Emission Services March All Notes Emission Services All Notes All No	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Miles Mile	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Miles Mile	Call Filesystem API	API Name: FindFirstFileFvW Arns: (%windir%\system32\WindowsPowerShell\v1 0\Modules\NetConnection* 0 h92e488 0 0 0 \N Return: ach5a08	2768	2220
Millander Harmon Millander Herbert And Programmer Millander Herbert And Programm				
March Marc				
Part				
Property And Prop	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\t^*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
A Prince of Prince	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Processing Content	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Marie Propriet Michael Affire Marie Four Flack Consult Supplication Affire Aff	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Marie Propriet Michael Affire Marie Four Flack Consult Supplication Affire Aff	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, b92e43c, 0, 0, 0) Return: acb5c88	2768	2220
Miles				
1971 1972				
Mile				
Miles Mile				
A Passer	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Properties A Prince Performance of the Comment	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\system 32 \ensuremath{\mbox{WindowsPowerShell}\mbox{V}1.0 \ensuremath{\mbox{Modules}\mbox{NetQos}\mbox{N}^*}, 0, b92e488, 0, 0, 0)\ Return: acb5a08 \ensuremath{\mbox{acb5a08}}$	2768	2220
AFF None Inchange AFF None Inchant Inchant Ang. (None Control (Control (Co	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
AP Note Principal Prin	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
California				
AFF Insert part AFF AFF Insert part part part part part part part pa				
Cal Floryton API				
Cell Pisagetian AF APP Name Profried Falco M Agr. (Nameth Visignami/Drivinous Proceedings 100 Modern Prof. 10 (100 May 10, 10) Name undoted 218 220		API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b92e43c, 0, 0, 0) Return: acb5a08		2220
Call Flaggerin AR	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b92e488, 0, 0, 0) Return: acb5b08	2768	2220
Calificacytion APP APP Name Profitable Wags (Norder-Volgstein-Zilvinder-Vorgethalt) (Abbodanishard Perf Pir 1, 150-468), 0, 0) Platim action (276	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ wwindir\% lsystem 32 \ Windows Power Shell \ 1.0 \ Modules\ Net TCPIP\ 1.0 \ Modules\ 1$	2768	2220
APT Note Professificial Section Age; (Normal Project Relative District Connective) Status P. (1925-00.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Cold Fleeystem AFT	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Cold Fleeystem AFT			2768	2220
Calificacystem API	can r necyclem r n		2.00	2220
Continue	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92e43c, 0, 0, 0) Return: acb5a	2768	2220
Part				
Call Filesystem APP	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b92e488, 0, 0, 0) Return: acb5c4	2768	2220
Call Fleeyplam API		8		
Call Filesystem AP API Name FindFirstFieEMW Ages (*Winderfisiopstem2WindowsPowerShelln/L OModules/Net/Co. 0, 0) Februm actidation 2768 220 220 Call Filesystem AP API Name FindFirstFieEMW Ages (*Winderfisiopstem2WindowsPowerShelln/L OModules/NCt), 0, 10054-100, 0, 0, 0) Februm actidation 2768 220 220 Call Filesystem AP API Name FindFirstFieEMW Ages (*Winderfisiopstem2WindowsPowerShelln/L OModules/NCt), 0, 10054-100, 0, 0, 0) Februm actidation 2768 220 220 Call Filesystem AP API Name FindFirstFieEMW Ages (*Winderfisiopstem2WindowsPowerShelln/L OModules/NCt), 0, 10054-100, 0, 0, 0) Februm actidation 2768 220 220 Call Filesystem AP API Name FindFirstFieEMW Ages (*Winderfisiopstem2WindowsPowerShelln/L OModules/NCt), 0, 10054-100, 0, 0, 0) Februm actidation 2768 220 220 Call Filesystem AP API Name FindFirstFieEMW Ages (*Winderfisiopstem2WindowsPowerShelln/L OModules/NCt), 0, 10054-100, 0, 0, 0) Februm actidation 2768 220 221 Call Filesystem AP API Name FindFirstFieEMW Ages (*Winderfisiopstem2WindowsPowerShelln/L OModules/NCt), 0, 10054-100, 0, 0, 0) Februm actidation 2768 220 221 Call Filesystem AP API Name FindFirstFieEMW Ages (*Winderfisiopstem2WindowsPowerShelln/L OModules/NCt), 0, 10054-100, 0, 0, 0) Februm actidation 2768 220 221 Call Filesystem AP API Name FindFirstFieEMW Ages (*Winderfisiopstem3ZWindowsPowerShelln/L OModules/NCt), 0, 10054-100, 0, 0, 0) Februm actidation 2768 220 221 Call Filesystem AP API Name FindFirstFieEMW Ages (*Winderfisiopstem3ZWindowsPowerShelln/L OModules/NCt), 0, 10054-100, 0, 0) Februm actidation 2768 220 222 Call Filesystem AP API Name FindFirstFieEMW Ages (*Winderfisiopstem3ZWindowsPowerShelln/L OModules/NCt), 0, 10054-100, 0, 0) Februm actidation 2768 220 222 Call Filesystem AP API Name FindFirstFieEMW Ages (*Winderfisiopstem3ZWindowsPowerShelln/L OModules/NCt), 0, 10054-100, 0, 0) Februm actidation 2768 220 222 Call Filesystem AP API Name FindF	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	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetworkTransition*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem AP AP Name FirdFirstFileSW Args: ("Naridef Noystem S2WIndowsPowerShell") (ModulesPKN*, 0.1824-35.0, 0.0) Fietum actication 2768 2200 2200 2200 2200 2200 2200 2200 22			2768	2220
Call Filesystem AP AP Name: FineFineFielE-W Agrs. (*windrik*)system/32WindowsPowerShelln/t (Modules/PKI*)*, 0.162c453, 0.0.0) Return actios68				
Call Filesystem API				
Call Filesystem AP AP Name: FindfiritsFileEXM Ags. (Windriksystem32WindowsPowerShellhr J. OModulesPhpDevicei*, 0, 192e45c, 0, 0, 0) Return: act6s08	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK*, 0, b92e43c, 0, 0, 0) Return: acb5c88	2768	2220
Call Filesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\PKI*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Cal Fleeystem API API Name: FindFirsiFileEXW Agrs. (%windri/kuystem32WindowsPowerShellyrl. OModulesiProManagement*)	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\PnpDevice*, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShelllv1.0Modules)PrintManagement*, 0, 862e43c, 0, 0, 0) Return: acb5608 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShellv1.0Modules)PrintManagement*, 0, 862e43c, 0, 0, 0) Return: acb5608 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShellv1.0Modules)PsDesiredStateConfiguration*, 0, b62e43c, 0, 0, 0) Return: acb5608 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShellv1.0Modules)PsDesiredStateConfiguration*, 0, b62e43c, 0, 0, 0) Return: acb 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShellv1.0Modules)PsDesiredStateConfiguration*, 0, b62e43c, 0, 0, 0) Return: acb5608 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShellv1.0Modules)PsDiagnostics*, 0, b62e43c, 0, 0, 0) Return: acb5608 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShellv1.0Modules)PsDiagnostics*, 0, b62e43c, 0, 0, 0) Return: acb5608 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShellv1.0Modules)PsDiagnostics*, 0, b62e43c, 0, 0, 0) Return: acb5608 278 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: (%windri%system3zWindowsPowerShelllv1.0Modules)PrintManagement*, 0, 862e43c, 0, 0, 0) Return: acb5608 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShellv1.0Modules)PrintManagement*, 0, 862e43c, 0, 0, 0) Return: acb5608 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShellv1.0Modules)PsDesiredStateConfiguration*, 0, b62e43c, 0, 0, 0) Return: acb5608 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShellv1.0Modules)PsDesiredStateConfiguration*, 0, b62e43c, 0, 0, 0) Return: acb 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShellv1.0Modules)PsDesiredStateConfiguration*, 0, b62e43c, 0, 0, 0) Return: acb5608 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShellv1.0Modules)PsDiagnostics*, 0, b62e43c, 0, 0, 0) Return: acb5608 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShellv1.0Modules)PsDiagnostics*, 0, b62e43c, 0, 0, 0) Return: acb5608 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShellv1.0Modules)PsDiagnostics*, 0, b62e43c, 0, 0, 0) Return: acb5608 278 2220	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\PnpDevice*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShelliv1.0Modules)PrintManagement*, 0, b82e43c, 0, 0, 0) Return: acb5688 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b82e43c, 0, 0, 0) Return: acb5688 2788 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b82e43c, 0, 0, 0) Return: acb5688 2788 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b82e48c, 0, 0, 0) Return: acb5608 2788 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b82e48c, 0, 0, 0) Return: acb5608 2788 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShelliv1.0Modules)PSDesignestics*), 0, b82e48c, 0, 0, 0) Return: acb5608 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShelliv1.0Modules)PSDesignestics*), 0, b82e48c, 0, 0, 0) Return: acb5608 278 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system3zWindowsPowerShelliv1.0Modules)PSDesignestics*), 0, b82e48c, 0, 0, 0) Return: acb5608 278 2220				
Call Fliesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0Modules)PSDesiredStateConfiguration**, 0, b92e43c, 0, 0, 0) Return: acb5c88 2768 2220 Call Fliesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0Modules)PSDesiredStateConfiguration**, 0, b92e43c, 0, 0, 0) Return: acb5 2768 2220 Call Fliesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0Modules)PSDesiredStateConfiguration**, 0, b92e43c, 0, 0, 0) Return: acb5 2768 2220 Call Fliesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0Modules)PSDesiredStateConfiguration**, 0, b92e48c, 0, 0, 0) Return: acb5 2768 2220 Call Fliesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0Modules)PSDiagnostica**, 0, b92e43c, 0, 0, 0) Return: acb5608 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0Modules)PSDiagnostica**, 0, b92e43c, 0, 0, 0) Return: acb5608 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0Modules)PSScheduled.ob**, 0, b92e43c, 0, 0, 0) Return: acb5608 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellV1.0Modules)PSScheduled.ob**)*, 0, b92e43c, 0, 0, 0) Return: acb5608 2768				
Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system32WindowsPowerShelllv1.0Modules)PSDesiredStateConfiguration*, 0, b92e43c, 0, 0, 0) Return: acb 508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system32WindowsPowerShelllv1.0Modules)PSDesiredStateConfiguration*, 0, b92e43c, 0, 0, 0) Return: acb 508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system32WindowsPowerShelllv1.0Modules)PSDesiredStateConfiguration*, 0, b92e48c, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system32WindowsPowerShelllv1.0Modules)PSDlagnostics*, 0, b92e48c, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system32WindowsPowerShelllv1.0Modules)PSDlagnostics*, 0, b92e48c, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system32WindowsPowerShelllv1.0Modules)PSScheduled.bbt*) 0, b92e48c, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system32WindowsPowerShellv1.0Modules)PSScheduled.bbt*) 0, b92e48c, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%system32WindowsPowerShellv1.0Modules)PSScheduled.bbt*) 0, b92e48c, 0, 0, 0) Return: acb508 2768 2220 </td <td>·</td> <td>• • • • • • • • • • • • • • • • • • • •</td> <td></td> <td></td>	·	• • • • • • • • • • • • • • • • • • • •		
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\PSDesiredStateConfiguration**, 0, b92e43c, 0, 0, 0) Return: acb 5a08 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\PSDesiredStateConfiguration**, 0, b92e48c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\PSDiagnostics**, 0, b92e43c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\PSDiagnostics**, 0, b92e48c, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\PSDiagnostics**, 0, b92e48c, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\PSScheduledJob**, 0, b92e48c, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\PSScheduledJob**, 0, b92e48c, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\PSScheduledTasks**, 0, b92e48c, 0, 0, 0) Return: acb508 2768 2220	•			
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b92e48a, 0, 0, 0) Return: acb 508 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b92e48a, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules)PSDiagnostics*, 0, b92e43c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules)PSDiagnostics*, 0, b92e48c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules)PSScheduledJob*, 0, b92e48c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules)PSScheduledJob*, 0, b92e48c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules)PSScheduledJob*, 0, b92e48c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules)PSScheduledJob*, 0, b92e48c, 0, 0, 0) Return: acb5008 2768 2220 Call	Call Filesystem API		2768	2220
6a08 Call Filesystem API 5a08 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration**, 0, b92e43c, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0Modules)PSDiagnosics**, 0, b92e43c, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0Modules)PSDiagnosics**, 0, b92e488, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0Modules)PSScheduledJob**, 0, b92e480, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0Modules)PSScheduledJob**, 0, b92e43c, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0Modules)PSScheduledJob**, 0, b92e43c, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0Modules)ScheduledTasks*), 0, b92e43c, 0, 0, 0) Return: acb508 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0Modules)ScheduledTask	Call Filosyctom API		2769	2220
API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\n'.0Modules\PSDesiredStateConfiguration\n', 0, b92e488, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\n'.0Modules\PSDiagnostics\n', 0, b92e43c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\n'.0Modules\PSDiagnostics\n', 0, b92e43c, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\n'.0Modules\PSDiagnostics\n', 0, b92e488, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\n'.0Modules\PSScheduledJob\n', 0, b92e48c, 0, 0, 0) Return: acb5048 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\n'.0Modules\PSScheduledJob\n', 0, b92e43c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\n'.0Modules\PSScheduledJob\n', 0, b92e43c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\n'.0Modules\PSScheduledJob\n', 0, b92e43c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\n'.0Modules\PSScheduledTasks\n', 0, b92e43c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\n'.0Modules\PScheduledTasks\n', 0, b92e43c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\n'.0Modules\PScheduledTasks\n', 0, b92e43c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\n'.0Modules\PScheduledTasks\n', 0, b92e43c, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args:	Call Filesystem API		2/00	2220
Sa88 5a88 Cal Fliesystem API API Name: FindfirstFileExW Args: (%windir%system32WindowsPowerShell\n1.0Modules\PSDiagnostics\n1, 0.b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Fliesystem API API Name: FindfirstFileExW Args: (%windir%system32WindowsPowerShell\n1.0Modules\PSDiagnostics\n1, 0.b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Fliesystem API API Name: FindfirstFileExW Args: (%windir%system32WindowsPowerShell\n1.0Modules\PSScheduledJob\n1, 0.b92e48c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindfirstFileExW Args: (%windir%system32WindowsPowerShell\n1.0Modules\PSScheduledJob\n1, 0.b92e48c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindfirstFileExW Args: (%windir%system32WindowsPowerShell\n1.0Modules\PSScheduledJob\n1, 0.b92e48c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindfirstFileExW Args: (%windir%system32WindowsPowerShell\n1.0Modules\PSScheduledJob\n1, 0.b92e48c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindfirstFileExW Args: (%windir%system32WindowsPowerShell\n1.0Modules\PScheduledTasks\n1, 0.b92e48c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindfirstFileExW Args: (%windir%system32WindowsPowerShell\n1.0Modules\PScheduledTasks\n1, 0.b92e48c, 0, 0, 0) Return: acb5a08 2768 <td>Call Filesystem ADI</td> <td></td> <td>2768</td> <td>2220</td>	Call Filesystem ADI		2768	2220
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tau, 0, 0, 0) Return: acb5008 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tau, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tau, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\tau, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\tau, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\tau, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\tau, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\tau, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesyste	Gall Filesystetti API		2100	2220
API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v1, 0, b92e488, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v1, 0, b92e488, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call F	Call Filesystem API		2768	2220
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob\v, 0, b92e43a, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v, 0, b92e43a, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v, 0, b92e43a, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v, 0, b92e43a, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PScheduledTasks\v1, 0, b92e43a, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PScheduledTasks\v1, 0, b92e43a, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PScureBool\v1, 0, b92e43a, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PScureBool\v1, 0, b92e43a, 0, 0, 0) Return: acb5a08 2768 2220 <tr< td=""><td></td><td></td><td></td><td></td></tr<>				
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, b92e48c, 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, b92e48c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b92e48c, 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, b92e48c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (\mathred{**windir\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, b92e48c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (\mathred{**windir\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, b92e48c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (\mathred{**windir\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, b92e48c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesyste				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks*, 0, b92e48c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\PSDiagnostics*, 0, b92e488, 0, 0, 0) Return: acb5a08		2220
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Scheduled\Job*, 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, 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, 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\Storage*, 0, b92e43c, 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\ScheduledTasks\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\v1, 0, b92e488, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\system 32 \end{\colorate} Windows Power Shell \end{\colorate} windir\% system 32 \end{\colorate} Windows Power Shell \end{\colorate} windir\% system 32 \end{\colorate} Windows Power Shell \end{\colorate} windir\% system 32 \col$	2768	2220
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\v1, 0, b92e488, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\v1, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\v1, 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\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220				2220
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\t^*, 0, b92e488, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220				
API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, b92e488, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, b92e48c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, b92e48c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, b92e48c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, b92e488, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Wodules\Storage*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Wodules\Storage*, 0, b92e43c, 0, 0, 0) Return: acb5a08 2768 2220	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ wwindir\%lsystem 32 \ Windows PowerShell \ v1.0 \ Modules\ SecureBoot \ v3.0,0,0)\ Return: acb 5a08$	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%lsystem32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 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: acb5a88 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
An i manife. I multiplume inclusive angle. (//wwindin //stystemoz/ivinuowsnoweronemy i.u/in/oudles/oudage(, 0, 092e406, 0, 0, 0) Return: acobato 2/06 2220	·	• • • • • • • • • • • • • • • • • • • •		
	Guii I ileayatetti At ^e l	79 TRAING, FINGUISH HELATY PAGE, (/WHITCH /otsystems/etyllidows/fowershelly Louwidules/staldget, U, 09/26400, U, U, U) Return: 8003808	2100	2220

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\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	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ system 32\ Windows PowerShell\ v1.0\ Modules\ Troubleshooting Pack\ v1.0\ Modules\ Troubleshooting Pack\ v1.0\ Modules\ v$	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\t^*, 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\VpnClien\t*, 0, b92e43c, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClien\t^*, 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: acb5a	2768	2220
	08		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, b92e43c, 0, 0, 0) Return: acb5c 48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, b92e488, 0, 0, 0) Return: acb5a 88	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\t^*, 0, b92e43c, 0, 0, 0) Return: acb5b08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\tag{*}, 0, b92e43c, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\t^*, 0, b92e488, 0, 0, 0) Return: acb5a08	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate\t^*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
		2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%)system32\WindowsPowerShellfv1.0\Modules\WindowsUpdate*, 0, b92e43c, 0, 0, 0) Return: acb5c48		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\WindowsUpdate\v1, 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#\dagger, 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 T ype: 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%MicrosoftWindows\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)%\WindowsPowerShellModules\PackageManagement*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShelf\Modules\PackageManagemenf\t, 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\tau, 0, b92e344, 0, 0, 0) Return: acb5c4 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0, 0, b92e344, 0, 0, 0) Return: acb5c4 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0\", 0, b92e390, 0, 0, 0) Return: acb5c4 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\tau^*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pestert*, 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\3.3.51*, 0, b92e344, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5\tau, 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)%\WindowsPowerShellModules\PowerShellGet*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGet*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API		2768	2220
· · · · · · · · · · · · · · · · · · ·	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGet*, 0, b92e488, 0, 0, 0) Return: acb5c48		
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules*, 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\%\ system 32\ \ Windows PowerShell \ \ 1.0\ \ \ Modules\ \ \ AppLocker\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	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
•	5		

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache\t^*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache\t^*, 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: ac b5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b92e43c, 0, 0, 0) Return: ac b5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b92e488, 0, 0, 0) Return: ac b5c48	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
		2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b92e43c, 0, 0, 0) Return: acb5c48		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient\t^*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient\t^*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b92e43c, 0, 0, 0) Return: acb5c4 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b92e43c, 0, 0, 0) Return: acb5c4 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b92e488, 0, 0, 0) Return: acb5c4 8	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\v*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS\i*, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS\i*, 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
		2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\\SE*, 0, b92e43c, 0, 0, 0) Return: acb5c48		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\\SE\\^0, 0, b92e43c, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\\SE*, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\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: acb5 c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b92e43c, 0, 0, 0) Return: acb5 c48	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: acb5 c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 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: acb5c4 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92e43c, 0, 0, 0) Return: acb5c4 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b92e488, 0, 0, 0) Return: acb5c4 8	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\v*, 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\v*, 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\t^*, 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: a b56x48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\v1, 0, b92e43c, 0, 0, 0) Return: a b56c48	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) R	2768	2220
Call Filesystem API	eturn: acb5c48 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e344, 0, 0, 0) R	2768	2220
Call Filesystem API	eturn: acb5c48 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b92e390, 0, 0, 0) R	2768	2220
Call Filesystem API	eturn: acb5c48 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b92e488, 0, 0, 0) Return: a	2768	2220
	cb5c48		

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b92e43c, 0, 0, 0) Return: acb 5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\t^*, 0, b92e43c, 0, 0, 0) Return: acb	2768	2220
Call Filesystem API	5c48 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\t^*, 0, b92e488, 0, 0, 0) Return: acb	2768	2220
Call Filesystem API	5048 ADD Nome: FindFindFileFilM Area / 9/usindis9/sustane23W6ndous/Deurschallt.d ()Mediulo/Microsoft Deurschallt Hillihat 0, 6004426, 0, 0, 0,) Pature: exhibit	2768	2220
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92e43c, 0, 0, 0) Return: acb5c 48		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92e43c, 0, 0, 0) Return: acb5c 48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b92e488, 0, 0, 0) Return: acb5c 48	2768	2220
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ system 32 \ Windows PowerShell \ v1.0 \ Modules \ Microsoft. WSMan, Management \ v1,0,692e43c,0,0,0)\ Return: ac b5c48$	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\t^*, 0, b92e43c, 0, 0, 0) Return: ac b5c48	2768	2220
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\t^*, 0, b92e488, 0, 0, 0) Return: ac b5c48	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
	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\MsDtc\t^, 0, b92e488, 0, 0, 0) Return: acb5c48	2768	
Call Filesystem API			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	$API\ Name: FindFirstFileExW\ Args: (\ windir\%\ system 32\ Windows Power Shell\ v1.0\ Modules\ Net Adapter\ v^*,\ 0,\ b92e488,\ 0,\ 0,\ 0)\ Return:\ acb5c48$	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%IMicrosoftlWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b5fd8f10-6d42-4d50-b6b5-afee3530516e Ty	2768	2220
	pe: VSDT_COM_DOS		
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%MicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_45a90088-863e-4343-b218-7fa1233240f8 T ype: 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 T ype: 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
		2768	
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_767a28c0-576a-468e-93b3-a92a5l4fa688 T ype: VSDT_COM_DOS		2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
		0700	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cdb97018-912e-4235-9409-7ef46e6a3455 T ype: VSDT_COM_DOS	2768	2220
Write File Write File		2768	2220
	ype: VSDT_COM_DOS		
Write File	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows)PowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows)PowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T	2768	2220
Write File Write File	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\)pipeIPSHost.133177542798913175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803	2768 2768	2220 2220
Write File Write File Call Filesystem API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\l\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Characteristic: Creates named pipe	2768 2768	2220 2220
Write File Write File Call Filesystem API Detection Write File	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 732 2768	2220 2220 844
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows)PowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows)PowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 732 2768 732	2220 2220 844 2220 844
Write File Write File Call Filesystem API Detection Write File Call System API Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows)PowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows)PowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 732 2768 732 732	2220 2220 844 2220 844 844
Write File Write File Call Filesystem API Detection Write File Call System API Call System API Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows)PowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows)PowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 732 2768 732 732 732	2220 2220 844 2220 844 844 844
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 732 2768 732 732 732 732	2220 2220 844 2220 844 844 844 844
Write File Write File Call Filesystem API Detection Write File Call System API Call System API Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows)PowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows)PowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 732 2768 732 732 732	2220 2220 844 2220 844 844 844
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 732 2768 732 732 732 732	2220 2220 844 2220 844 844 844 844
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindows)PowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindows)PowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 732 2768 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844
Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\l\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Characteristic: Creates named pipe \l\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: GetDriveTypeW Args: (D:\) Return: 5	2768 2768 732 2768 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\l\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Characteristic: Creates named pipe \l\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell Path: %LOCALAPPDATA%iMicrosoftiWindows\PowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: GetDriveTypeW Args: (D:\) Return: 5 API Name: GetDriveTypeW Args: (D:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2	2768 2768 732 2768 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844 844
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\l\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Characteristic: Creates named pipe \l\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: GetDriveTypeW Args: (D:\) Return: 5 API Name: GetDriveTypeW Args: (E:\) Return: 2	2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844 844 844
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\l\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Characteristic: Creates named pipe \l\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: GetDriveTypeW Args: (D\L) Return: 5 API Name: GetDriveTypeW Args: (D\L) Return: 5 API Name: GetDriveTypeW Args: (D\L) Return: 5 API Name: GetDriveTypeW Args: (E\L) Return: 2	2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844 844 844 844 844
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\l\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844 844 844 844 844 84
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Characteristic: Creates named pipe \\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: GetDriveTypeW Args: (DA) Return: 5 API Name: GetDriveTypeW Args: (EA) Return: 2	2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844 844 844 844 844 8
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%IMicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%IMicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Characteristic: Creates named pipe \\\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell Path: %LOCALAPPDATA%IMicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: GetDriveTypeW Args: (D\\) Return: 5 API Name: GetDriveTypeW Args: (D\\) Return: 5 API Name: GetDriveTypeW Args: (D\\) Return: 5 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (F\\) Return: 2 API Name: GetDriveTypeW Args: (F\\) Return: 2 API Name: GetDriveTypeW Args: (F\\) Return: 2 API Name: GetDriveTypeW Args: (F\\) Return: 2 API Name: GetDriveTypeW Args: (F\\) Return: 2 API Name: GetDriveTypeW Args: (F\\) Return: 2	2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844 844 844 844 844 8
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Characteristic: Creates named pipe \\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: GetDriveTypeW Args: (DA) Return: 5 API Name: GetDriveTypeW Args: (EA) Return: 2	2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844 844 844 844 844 8
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%IMicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%IMicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Characteristic: Creates named pipe \\\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell Path: %LOCALAPPDATA%IMicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: GetDriveTypeW Args: (D\\) Return: 5 API Name: GetDriveTypeW Args: (D\\) Return: 5 API Name: GetDriveTypeW Args: (D\\) Return: 5 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (E\\) Return: 2 API Name: GetDriveTypeW Args: (F\\) Return: 2 API Name: GetDriveTypeW Args: (F\\) Return: 2 API Name: GetDriveTypeW Args: (F\\) Return: 2 API Name: GetDriveTypeW Args: (F\\) Return: 2 API Name: GetDriveTypeW Args: (F\\) Return: 2 API Name: GetDriveTypeW Args: (F\\) Return: 2	2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844 844 844 844 844 8
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-db87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844 844 844 844 844 8
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844 844 844 844 844 8
Write File Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindows)PowerShell(CommandAnalysis)PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindows)PowerShell(CommandAnalysis)PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\pipe)PSHost.133177542798913175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Characteristic: Creates named pipe \\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell Path: %LOCALAPPDATA%MicrosoftWindows)PowerShell(CommandAnalysis)PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: GetDriveTypeW Args: (DA) Return: 5 API Name: GetDriveTypeW Args: (DA) Return: 5 API Name: GetDriveTypeW Args: (DA) Return: 5 API Name: GetDriveTypeW Args: (EA) Return: 2 API Name: GetDriveTypeW Args: (EA) Return: 2	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 2220 844 844 844 844 844 844 844 844 844 84
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\Power\Shell\CommandAnalysis\Power\Shell_Analysis\CacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\Power\Shell\CommandAnalysis\Power\Shell_Analysis\CacheInty. d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Characteristic: Creates named pipe \\\pipe\PSHost.133177542798913175.844.DefaultAppDomain.powershell Path: %LOCALAPPDATA%\Microsoft\Windows\Power\Shell\CommandAnalysis\Power\Shell_Analysis\CacheIndex Type: VSDT_COM_DOS API Name: GetDriveTypeW Args: (D:\) Return: 5 API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 5	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844 844 844 844 844 8
Write File Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%:MicrosoftWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%:MicrosoftWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844
Write File Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%:MicrosoftWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%:MicrosoftWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\(\) ippeiPSHost.133177542798913175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Characteristic: Creates named pipe \(\) ippeiPSHost.133177542798913175.844.DefaultAppDomain.powershell \(\) Path: %LOCALAPPDATA%:MicrosoftWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS \(\) API Name: GetDriveTypeW Args: (D\(\)) Return: 5 \(\) API Name: GetDriveTypeW Args: (D\(\)) Return: 5 \(\) API Name: GetDriveTypeW Args: (D\(\)) Return: 5 \(\) API Name: GetDriveTypeW Args: (D\(\)) Return: 5 \(\) API Name: GetDriveTypeW Args: (D\(\)) Return: 5 \(\) API Name: GetDriveTypeW Args: (D\(\)) Return: 2 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 2 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 2 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 2 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 2 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 2 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 2 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 2 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 2 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 2 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 2 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 2 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 2 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 5 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 5 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 5 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 5 \(\) API Name: GetDriveTypeW Args: (E\(\)) Return: 5 \(\) API Name: Get	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844
Write File Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShellCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShellCommandAnalysisiPowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bb8 T ype; VSDT_COM_DOS API Name: CreateNamedPipeW Args: (1 lipiePIPSHost.133177542798913175.844.DefaultAppDomain.powershell. 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Characteristic: Creates named pipe \(\) \(\	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Patt: %LOCALAPPDATA%MicrosoftWindowsPowerShell(CommandAnalysis)PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Patt: %LOCALAPPDATA%MicrosoftWindowsPowerShell(CommandAnalysis)PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 Typee: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844
Write File Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShellCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShellCommandAnalysisiPowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bb8 T ype; VSDT_COM_DOS API Name: CreateNamedPipeW Args: (1 lipiePIPSHost.133177542798913175.844.DefaultAppDomain.powershell. 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Characteristic: Creates named pipe \(\) \(\	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Patt: %LOCALAPPDATA%MicrosoftWindowsPowerShell(CommandAnalysis)PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Patt: %LOCALAPPDATA%MicrosoftWindowsPowerShell(CommandAnalysis)PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 Typee: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsPowerShellCommandAnalysisPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsPowerShellCommandAnalysisPowerShell_AnalysisCacheEntry_d56a8518.615b-4c03-b126-4b87cf95bb8 Type: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (1\pipe)PSHost.133177542789813175.844.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803 516) Return: 548 Threat Chraracteristic: Creates named pipe 1\pipe)PSHost.133177542788913175.844.DefaultAppDomain.powershell Path: %LOCALAPPDATA%MicrosoftWindowsPowerShellCommandAnalysisPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: GetDirveTypeW Args: (DA) Return: 5 API Name: GetDirveTypeW Args: (CA) Return: 5 API Name: GetDirveTypeW Args: (CA) Return: 2	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShellCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShellCommandAnalysisiPowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b57c95bb8 T ype: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (1\pipe)PSHost.133177542798913175.844 DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 10803 516 Return: 548 Threat Characteristic: Creates named pipe 1\pipe)PSHost.133177542798913175.844.DefaultAppDomain.powershell Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShellCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: GetDriveTypeW Args: (D\) Return: 5 API Name: GetDriveTypeW Args: (E\) Return: 2 API Name	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsPowerShellCommandAnalysisPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsPowerShellCommandAnalysisPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: CreateNamedPipeW Args: (1\)pie/PSHost.133177542798913175.844 DefaultAppDomain.powershell, 1074268115, 6, 1, 32768, 32768, 0, 10803 API Name: CreateNamedPipeW Args: (1\)pie/PSHost.133177542798913175.844 DefaultAppDomain.powershell, 1074268115, 6, 1, 32768, 32768, 0, 10803 Threat Characteristic: Creates named pipe \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844 844 844 844 844 84
Write File Write File Call Filesystem API Detection Write File Call System API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShellCommandAnalysisiPowerShell_AnalysisCacheEntry_d56a8518-6150-LOO3-b126-4b87c95b86 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShellCommandAnalysisiPowerShell_AnalysisCacheEntry_d56a8518-6150-4c03-b126-4b87c95b86 T ype: VSDT_COM_DOS API Name: CreateNamediPipeW Args: (Ni_pipePSHost.133177542798913175.844.DefaultAppDomain.powershell_1074266115, 6, 1, 32768, 32768, 0, 10803 5165) Return: 518 Threat Characteristic: Creates named pipe Ni_pipePSHost.133177542798913175.844 DefaultAppDomain.powershell Particle Characteristic: Creates named pipe Ni_pipePSHost.133177542798913175.844 DefaultAppDomain.powershell Particle Particl	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844 844 844 844 844 84
Write File Write File Call Filesystem API Detection Write File Call System API Call System API	yper VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShellCommandAnalysisPowerShell_AnalysisCachelEntry_d56a8518-615b-4c03-b126-4b87cf95bth8 T yper VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShellCommandAnalysisPowerShell_AnalysisCachelEntry_d56a8518-615b-4c03-b126-4b87cf95bth8 T yper VSDT_COM_DOS API Name: CreateNamedPipeW Args: (\(\) \	2768 2768 2768 732 2768 732 732 732 732 732 732 732 732 732 732	2220 2220 844 2220 844 844 844 844 844 844 844 844 844 84

Designation				
March (American all Control (American American Ameri	Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	732	844
March (American all Control (American American Ameri	Call System API	API Name: GetDriveTypeW Args; (C:\Users\) Return: 3	732	844
Month Month State And The Month State S				
### 1987年				
Month Mont	Write File	Path: %TEMP%\cyax2su.2xq.ps1 Type: VSDT_ASCII		844
Districture of the Control o	Add File	Path: %TEMP%\i024mgn.5ve.psm1 Type: VSDT_ASCII	732	844
1987年 日本	Write File	Path: %TEMP%\li024mgn.5ve.psm1 Type: VSDT_ASCII	732	844
Process	Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%lcyax2su.2xq.ps1) Return: 1	732	844
Minute M	Delete File	Path: %TEMP%\cyax2su.2xq.ps1 Type: VSDT_ASCII	732	844
Property	Detection			
Page	Detection			
		File: %TEMP%\cyax2su.2xq.ps1		
Part		Type: VSDT_ASCII		
Part	Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\li024mgn.5ve.psm1) Return: 1	732	844
Process Proc	Delete File	Path: %TEMP%\ii024mgn.5ve.psm1 Type: VSDT_ASCII	732	844
Process Proc	Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
Time				
March Color March Color Colo				
March Marc				
Page	Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	732	844
March Proceed Proceed Proceed Proced	Call Service API	API Name: OpenServiceW Args: (7ca8e90, CryptSvc, 5) Return: 7ca8e18	732	844
March Path MacConferent Analysis and Content Analysis and Path MacConferent Analysis and Pa	Write File	$Path: \label{localAPPDATA} $$\operatorname{PowerShell}_{Analysis} PowerShell_{Analysis} Cache Entry_74f3b07c-765d-438c-a907-70d2693f4860\ T$$ $$\operatorname{PowerShell}_{Analysis} PowerShell_{Analysis} PowerShell_{Analysis} PowerShell_{Analysis} PowerShell_{Analysis} PowerShell_{Analysis} PowerShell_{Analysis} PowerShell_{Analy$	2768	2220
Part		ype: VSDT_COM_DOS		
Page	Write File	$Path: \&LOCALAPPDATA \&lMicrosoft \\ Windows \\ Power Shell \\ Command Analysis \\ Power Shell \\ Analysis \\ Cache \\ Index Type: VSDT_COM_DOS \\ Analysis \\ Command \\ Analysis \\ Comman$	2768	2220
Part	Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d3834826-5ebb-4133-88de-b2d88f8d76de	2768	2220
Miles				
A Prisone Prisonal Prisone A Prisone Priso	Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
A Prisone Prisonal Prisone A Prisone Priso	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lassembly\NativeImages v4.0.30319 32\System.Configuration*. 0. a4a9d0. 0. 0. 0) Return: ada9330	732	844
Part	·			
Coligonary All Polision Colification Polision Colification Polision Colification Polision Colification Polision Colification Polision Colification Polision Colification Polision		0 1 1		
A State				
APP Name Part P	Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	732	844
March Marc	Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	732	844
APT Notes Professional And APT Notes Professional News National Professional And APT Notes Professional News National Professional News National Professional News National Professional News National Professional Profe	Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	732	844
April Easystem APP APP Heaves Facilitation April Approx App	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules*, 0, ba3e7b4, 0, 0, 0) Return: ada9370	732	844
April Easystem APP APP Heaves Facilitation April Approx App	Call Filesystem API	API Name: FindNeytFileW Arns: (ada9370 ha3e7c4) Return: 1	732	844
Call Picopitan API	·			
API Norme Find Find Find Wager (New Individuo passens Strummune passens bell in 2004 Activation (p. 0.0.1) Passens addition (2004 Activation (p. 0.0.1) Passens addition (p. 0.0.1) Pas				
Cell Filesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\AppLocker*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Flowyshm API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Flasystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\AppLocker*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filosystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filosystem API	Call Filesystem API	API Name: FindFirstFileExW Aros: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, ba3e6bc, 0, 0, 0) Return; ada93f0	732	844
Call Pilesystem APP			732	844
Call Fleeystem AP API Name FindFristFieEW Apic (Nondrifs)system/Zuinfoxespowershelt in J. OModules/Bis Transfer**, 0, basiction, 0, 0, 0 Return action770 732 844				
Call Filesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, ba3e6bc, 0, 0, 0) Return: ada93/0	732	844
Call Filesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	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	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	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, ba3e6bc, 0, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API			732	844
Call Fleeystem API	·			
Call Filesystem API				
Call Fliesystem API API Name: FindFirstFileExW Args: (%windri%laystem32/windowspowershellv1.0ModulesiDirectAccessClientComponentsi*, 0, ba3eBbc, 0, 0, 0) Return: ada3370 844 Call Fliesystem API API Name: FindFirstFileExW Args: (%windri%laystem32/windowspowershellv1.0ModulesiDirectAccessClientComponentsi*, 0, ba3eBbc, 0, 0, 0) Return: ada3370 732 844 Call Fliesystem API API Name: FindFirstFileExW Args: (%windri%laystem32/windowspowershellv1.0ModulesiDirectAccessClientComponentsi*, 0, ba3eBbc, 0, 0, 0) Return: ada3370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%laystem32/windowspowershellv1.0ModulesiDirect), 0, ba3eBbc, 0, 0, 0) Return: ada3370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%laystem32/windowspowershellv1.0ModulesiDirect), 0, ba3eBbc, 0, 0, 0) Return: ada3370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%laystem32/windowspowershellv1.0ModulesiDirect), 0, ba3eBbc, 0, 0, 0) Return: ada3370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%laystem32/windowspowershellv1.0ModulesiDirect), 0, ba3eBbc, 0, 0, 0) Return: ada3370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windri%laystem32/windowspowershellv1.0ModulesiDirect), 0, ba3eBbc, 0, 0, 0) Return: ada3370 732 844 Call Filesystem API AP	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelllv1.0\Modules\CimCmdlets*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
API Name: FindFirstFielExW Args: (%windir%system32windowspowershelliv1.0ModulesiDirectAccessClientComponents**, 0, ba3e6bc, 0, 0, 0) Return: add 370	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\CimCmdlets\t^*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Fleeystem API API Name: FindFirsFieExW Args: (%windfi/klysystem32/windowspowershellv1.0ModulesiDirectAccessClientComponents)*, 0, ba3e6bc, 0, 0, 0) Return: add 370 844 Call Fleeystem API API Name: FindFirsFieExW Args: (%windfi/klysystem32/windowspowershellv1.0ModulesiDirectAccessClientComponents)*, 0, ba3e708, 0, 0, 0) Return: add3370 732 844 Call Fleeystem API API Name: FindFirsFieExW Args: (%windfi/klysystem32/windowspowershellv1.0ModulesiDism*, 0, ba3e708, 0, 0, 0) Return: add3370 732 844 Call Fleeystem API API Name: FindFirsFieExW Args: (%windfir/klysystem32/windowspowershellv1.0ModulesiDism*, 0, ba3e708, 0, 0, 0) Return: add3370 732 844 Call Fleeystem API API Name: FindFirsFieExW Args: (%windfir/klysystem32/windowspowershellv1.0ModulesiDism*, 0, ba3e6bc, 0, 0, 0) Return: add3370 732 844 Call Fleeystem API API Name: FindfirsFieExW Args: (%windfir/klysystem32/windowspowershellv1.0ModulesiDismClient*, 0, ba3e6bc, 0, 0, 0) Return: add3370 732 844 Call Fleeystem API API Name: FindfirsFieExW Args: (%windfir/klysystem32/windowspowershellv1.0ModulesiDismClient*, 0, ba3e6bc, 0, 0, 0) Return: add3370 732 844 Call Fleeystem API API Name: FindfirsFieExW Args: (%windfir/klysystem32/windowspowershellv1.0ModulesiExwertTracingManagement*, 0, ba3e6bc, 0, 0, 0) Return: add3370 732 844 Call Fleeystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e6bc, 0, 0, 0) Return: ad	732	844
API Name: FindFirstFileExW Args: (%windir%isystem32windowspowershellrv1.0Modules)DirectAccessClientComponents**, 0, ba3e708, 0, 0, 0) Return: ada9370		a9370		
Call Fliesystem API API Name: FindFirsiFileExW Args: (%windir%lsystem32windowspowershelliv1.0ModulesiDismi*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Fliesystem API API Name: FindFirsiFileExW Args: (%windir%lsystem32windowspowershelliv1.0ModulesiDismi*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Fliesystem API API Name: FindFirsiFileExW Args: (%windir%lsystem32windowspowershelliv1.0ModulesiDismi*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirsiFileExW Args: (%windir%lsystem32windowspowershelliv1.0ModulesiDismi*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirsiFileExW Args: (%windir%lsystem32windowspowershelliv1.0ModulesiDisnClienti*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirsiFileExW Args: (%windir%lsystem32windowspowershellv1.0ModulesiDisnClienti*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirsiFileExW Args: (%windir%lsystem32windowspowershellv1.0ModulesiDisnClienti*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirsiFileExW Args: (%windir%lsystem32windowspowershellv1.0ModulesiDisnCrienti*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirsiFileExW Args: (%wi	Call Filesystem API		732	844
Call Filesystem API API Name: FindFirstFileEXW Args: (%windir%isystem32/windowspowershelltv1.0ModulesIDism*r, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileEXW Args: (%windir%isystem32/windowspowershelltv1.0ModulesIDism*r, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileEXW Args: (%windir%isystem32/windowspowershelltv1.0ModulesIDism*r, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileEXW Args: (%windir%isystem32/windowspowershelltv1.0ModulesIDmsClient*r, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileEXW Args: (%windir%isystem32/windowspowershelltv1.0ModulesIDmsClient*r, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileEXW Args: (%windir%isystem32/windowspowershelltv1.0ModulesIDmsClient*r, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileEXW Args: (%windir%isystem32/windowspowershelltv1.0ModulesIDmsClient*r, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileEXW Args: (%windir%isystem32/windowspowershelltv1.0ModulesiDexertTracingManagement*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: Fi		a9370		
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0Modules\Dismi*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0Modules\Dismi*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0Modules\Dismi*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0Modules\Discilent*), 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0Modules\DracClient*), 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindfirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0Modules\DracClient*), 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindfirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0Modules\DracClient*), 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindfirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0Modules\DracClientTracingManagement*), 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API	Call Filesystem API		732	844
Call Flesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershelliv1.0Modules\Dismir 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershelliv1.0Modules\Dismir 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershelliv1.0Modules\DrsClient 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershelliv1.0Modules\DrsClient 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershelliv1.0Modules\DrsClient 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershelliv1.0Modules\DrsClient 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershelliv1.0Modules\DrsClient 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/windowspowershelliv1.0Modules\DrsClient 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args:		a9370		
Call Fliesystem API API Name: FindFirstFileExW Args: (%windir%system32lwindowspowershelliv1.0Modules)Dism'r, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lwindowspowershelliv1.0Modules)DnsClient*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lwindowspowershelliv1.0Modules)DnsClient*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lwindowspowershelliv1.0Modules)EventTracingManagement*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lwindowspowershelliv1.0Modules)EventTracingManagement*, 0, ba3e706, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lwindowspowershelliv1.0Modules)EventTracingManagement*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lwindowspowershelliv1.0Modules)EventTracingManagement*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lwindowspowershelliv1.0Modules)International*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesy	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%lsystem32\windowspowershelliv1.0\Modules\DnsClientl*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelliv1.0\Modules\DnsClientl*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\DnsClientl*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\EventTracingManagementl*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\EventTracingManagementl*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershellIv1.0\Modules\EventTracingManagementl*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershellIv1.0\Modules\International*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershellIv1.0\Modules\International*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\%) system 32 \ windows power shell \ v1.0 \ Modules\ Dism \ ^*, 0, ba 3e6bc, 0, 0, 0)\ Return: ada9370$	732	844
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellIv1.0\Modules\DnsClient\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellIv1.0\Modules\DnsClient\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellIv1.0\Modules\DnsClient\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellIv1.0\Modules\EventTracingManagement\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellIv1.0\Modules\EventTracingManagement\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellIv1.0\Modules\EventTracingManagement\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellIv1.0\Modules\International\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellIv1.0\Modules\International\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 <td>Call Filesystem API</td> <td>API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Dism*, 0, ba3e708, 0, 0, 0) Return: ada9370</td> <td>732</td> <td>844</td>	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Dism*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API API Name: FindFirstFileExW Ags: (%windir%system32windowspowershelliv1.0!ModulesiDnsClient1*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32windowspowershelliv1.0!ModulesiDnsClient1*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32windowspowershelliv1.0!ModulesiEventTracingManagement1*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32windowspowershelliv1.0!ModulesiEventTracingManagement1*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32windowspowershellIv1.0!ModulesiInternational1*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32windowspowershellIv1.0!ModulesiInternational1*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32windowspowershellIv1.0!ModulesiInternational1*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32windowspowershellIv1.0!ModulesiScSIN*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API <td></td> <td></td> <td>732</td> <td>844</td>			732	844
API Name: FindFirstFileExW Args: (%windir% system32\windowspowershelliv1.0\Modules\Londowspowershelliv1.0\modules\Londowspo				
API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\EventTracingManagement\t^, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\EventTracingManagement\t^, 0, ba3e6bc, 0, 0, 0) Return: ada9400 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\EventTracingManagement\t^, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\International\t^, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\International\t^, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\International\t^, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\ISCSI\t^, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\ISCSI\t^, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\ISCSI\t^, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\ISCSI\t^, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\ISCS\t^, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershelliv1.0lModules\ISC\t^, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32lw				
API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\EventTracingManagement*, 0, ba3e6bc, 0, 0, 0) Return: ada9450 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\EventTracingManagement*, 0, ba3e708, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International*, 0, ba3e708, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (%windir\system32\windowspowershell\v1.0\Modules\ISCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (\mindir\system32\windowspowershell\v1.0\Modules\ISCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (\mindir\system32\windowspowershell\v1.0\Modules\ISCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (\mindir\system32\windowspowershell\v1.0\Modules\ISCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (\mindir\system32\windowspowershell\v1.0\Modules\ISCS*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (\mindir\system32\windowspowershell\v1.0\Modules\ISCS*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (\mindir\system32\windowspowershell\v1.0\Modules\ISCS*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (\mindir\system32\windowspowershell\v1.0\Modules\ISCS*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\leventTracingManagement\v1, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\lnternational\v1, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\lnternational\v1, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\lnternational\v1, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\lsCSI\v1, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\lsCSI\v1, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\lsCSI\v1, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\lsCSI\v1, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\lsCSI\v1, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\lsCSI\v2, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\lsCSI\v2, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\lsCSI\v2, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\EventTracingManagement\t^*, 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, 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\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, 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\ISCS*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (\\$\windir\\system32\windowspowershell\v1.0\Modules\ISC*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (\\$\windir\\system32\windowspowershell\v1.0\Modules\ISC*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (\\$\windir\\system32\windowspowershell\v1.0\Modules\ISC*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (\\$\windir\\system32\windowspowershell\v1.0\Modules\ISC\S*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\%) system 32 \ windows power shell \ v1.0 \ Modules \ Event Tracing Management \ v, 0, ba 3e6bc, 0, 0, 0)\ Return: ada94b0$	732	844
API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelllv1.0!Modules\International*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelllv1.0!Modules\International*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelllv1.0!Modules\International*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelllv1.0!Modules\ISCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelllv1.0!Modules\ISCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelllv1.0!Modules\ISCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelllv1.0!Modules\ISCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelllv1.0!Modules\ISCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelllv1.0!Modules\ISCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelllv1.0!Modules\ISCS*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelllv1.0!Modules\ISCS*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0!Modules\ISCS*, 0, ba3e708, 0, 0, 0) Return: ada9370 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\windowspowershelliv1.0!Modules\International*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0!Modules\International*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0!Modules\ISCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershelliv1.0!Modules\ISCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershell\v1.0!Modules\ISE\ISE*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershell\v1.0!Modules\ISE\ISE*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershell\v1.0!Modules\ISE\ISE*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\windowspowershell\v1.0!Modules\ISE\ISE*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844	Call Filesystem API		732	844
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0!Modules\International*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0!Modules\iSCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0!Modules\iSCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0!Modules\iSCSI*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0!Modules\iSE\iSE*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0!Modules\iSE\iSE*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0!Modules\iSE\iSE*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0!Modules\iSCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0!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\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: ada9370 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\windowspowershelliv1.0!Modules\iSCSI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0!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: ada9370 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\\SCS\\^*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (\text{ windir}\system32\windowspowershell\v1.0\Modules\\SE\\^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (\text{ windir}\system32\windowspowershell\v1.0\Modules\\SE\\^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (\text{ windir}\system32\windowspowershell\v1.0\Modules\\SE\\^*, 0, ba3e708, 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\windowspowershelliv1.0!Modules\lSE 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0!Modules\lSE 0, ba3e6bc, 0, 0, 0) Return: ada9370 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0!Modules\lSE 0, ba3e708, 0, 0, 0) Return: ada9370 732 844	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\%) system 32 windows power shell to 1.0 tModules \ SCSIt^*, 0, ba3e6bc, 0, 0, 0)\ Return: ada9370$	732	844
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\\SE\^*, 0, ba3e6bc, 0, 0, 0) Return: ada93f0 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\\SE\^*, 0, ba3e708, 0, 0, 0) Return: ada93f0 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\\SE*, 0, ba3e6bc, 0, 0, 0) Return: ada93f0 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\\SE*, 0, ba3e708, 0, 0, 0) Return: ada93f0 732 844	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\\SE*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\\SE*, 0, ba3e708, 0, 0, 0) Return: ada9370 732 844				

Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\lModules\lKds\\)*, 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, 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: ada9 370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada9 370	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\v1, 0, ba3e708, 0, 0, 0) Return: ada9 370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e6bc, 0, 0, 0) Return: a da9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e6bc, 0, 0, 0) Return: a da93f0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e708, 0, 0, 0) Return: a da9370	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\t^*, 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\t^*, 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: ad a94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^*, 0, ba3e6bc, 0, 0, 0) Return: ad a94b0	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) Ret um: 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) Ret um: 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) Ret um: 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: ad a9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada9 370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e6bc, 0, 0, 0) Return: ada9 370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e708, 0, 0, 0) Return: ada9 370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e6bc, 0, 0, 0) Return: ada94b 0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e6bc, 0, 0, 0) Return: ada937 0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e708, 0, 0, 0) Return: ada937 0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada 9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e6bc, 0, 0, 0) Return: ada 9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e708, 0, 0, 0) Return: ada 9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\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\dagger, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NelConnection*, 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%lsystem32\windowspowershelllv1.0lModuleslNetConnection*, 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%lsystem32\windowspowershell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\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\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetLbfo\t^*, 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%lsystem32\windowspowershell\v1.0\)Modules\Net\Nat*, 0, ba3e6bc, 0, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Net\Nat\%, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Net\Nat*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: Find First File ExW Args: (%windir%lsystem32\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: ada94b 0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e708, 0, 0, 0) Return: ada94b	732	844
	0		
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%lsystem32\windowspowershell\v1.0\Modules\NetworkTransition*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetworkTransition*, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\PKI*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\PKI*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\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\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PrintManagement\t^*, 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: ada9 370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e6bc, 0, 0, 0) Return: ada9	732	844
	370		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e708, 0, 0, 0) Return: ada9 370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDiagnostics\t^*, 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%lsystem32\windowspowershell\v1.0\Modules\ScheduledTasks*, 0, ba3e708, 0, 0, 0) Return: ada93f0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\SecureBoot\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot\t^*, 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\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Storage*, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\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%lsystem32\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\t^*, 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\t, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%)system32\windowspowershell\v1.0\Modules\VpnClient\v1, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system32\windowspowershell\v1.0\Modules\VpnClient\t, 0, ba3e708, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%)system32\windowspowershell\v1.0\Modules\Wdac\v1, 0, ba3e6bc, 0, 0, 0) Return: ada9370	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%)system32\windowspowershell\v1.0\Modules\Wdac\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%)system32\windowspowershell\v1.0\Modules\Wdac\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Wdac\t^*, 0, ba3e708, 0, 0, 0) Return: ada9370 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Windowspowershell\v1.0\Modules\	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsDeveloperLicense\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada937 0	102	U***
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
0.1157	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShelf\Modules\PackageManagement\1.0.0.0*, 0, ba3e5c4, 0, 0, 0) Return: ada93f	732	844
Call Filesystem API	0		
Call Filesystem API Call Filesystem API	O 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\3.3.51*, 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\3.3.51*, 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)%WindowsPowerShellModules\PowerShellGet*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGet*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGett*, 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
· · · · · · · · · · · · · · · · · · ·		732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules*, 0, ba3e7b4, 0, 0, 0) Return: ada94b0		
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%lsystem32\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
			844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0lModules\Appx*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	
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\BitsTransfert*, 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\BitsTransfen*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\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%lsystem32\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: a da94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e6bc, 0, 0, 0) Return: a da94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e708, 0, 0, 0) Return: a	732	844
	da94b0		
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%lsystem32\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\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\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\WindowsPowerShelllv1.0\Modules\EventTracingManagement*, 0, ba3e6bc, 0, 0, 0) Return: ada94b 0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e6bc, 0, 0, 0) Return: ada94b 0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e708, 0, 0, 0) Return: ada94b 0	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
	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: Find Fishelexw Args: (%windir%system32)windowsPowerSneliw Luwodules\(\text{international\(\text{i}\), 0, ba3eobc, 0, 0, 0 \) Return: ada9460	132	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1. 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS\l^*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0lModules\iSCS(\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\lSE*, 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
•		732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732 732	844 844
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\ISE*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Idsh\ds\s', 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732 732 732	844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732 732	844 844
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\ISE*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Idsh\ds\s', 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732 732 732	844 844 844
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\ISE*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732 732 732 732	844 844 844 844
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\ISE*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732 732 732 732 732	844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\USE*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732 732 732 732 732 732	844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\USE*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Use\User\User\User\User\User\User\Use	732 732 732 732 732 732 732	844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\ISE*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell\Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell\Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell\Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell\Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732 732 732 732 732 732 732 732	844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE\\\^, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds\\\^, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds\\\^, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds\\\^, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive\\\^, 0, ba3e6bc, 0, 0, 0) Return: ada 94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive\\\^, 0, ba3e6bc, 0, 0, 0) Return: ada 94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive\\\^, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive\\\^, 0, ba3e5c4, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive\\\^, 0, ba3e5c4, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive\\\\^, 0, ba3e5c4, 0, 0, 0) Return: ada94b0	732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE\\^, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds\\^, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds\\^, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds\\^, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive\\^, 0, ba3e6bc, 0, 0, 0) Return: ada 94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive\\^, 0, ba3e6bc, 0, 0, 0) Return: ada 94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive\\^, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive\\^, 0, ba3e5c4, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive\\^, 0, ba3e5c4, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive\\^, 0, ba3e610, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.Archive\\^, 0, ba3e708, 0, 0, 0) Return: ada94b0	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\MsE¹*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Msds¹*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Msds¹*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Msds¹*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Microsoft.PowerShell.Archive**, 0, ba3e6bc, 0, 0, 0) Return: ada 94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive**, 0, ba3e6bc, 0, 0, 0) Return: ada 94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive**, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive**en-US**, 0, ba3e5c4, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive**en-US**, 0, ba3e610, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive**en-US**, 0, ba3e610, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive**en-US**, 0, ba3e60c, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics**, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\MsE¹*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Msds¹*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Msds¹*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Msdrs²*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Microsoft.PowerShell.Archive**, 0, ba3e6bc, 0, 0, 0) Return: ada 94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive**, 0, ba3e6bc, 0, 0, 0) Return: ada 94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive**, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive**, 0, ba3e5c4, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive**, 0, ba3e610, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive**, 0, ba3e610, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive**, 0, ba3e60c, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics**, 0, ba3e60c, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics**, 0, ba3e60c, 0, 0, 0) Return: ada94b0	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\MsE¹*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Msds¹*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Msds¹*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Msds¹*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada 94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada 94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3e5c4, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3e5c4, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3e610, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Msir, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Msir, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Msir, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Msir, 0, ba3e708, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada 94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada 94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3e5c4, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3e5c4, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3e708, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\t^*, 0, ba3e708, 0, 0, 0) Return: ada94b 0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\\Modules\Microsoft.PowerShell.Management\v1, 0, ba3e6bc, 0, 0, 0) Return	732	844
0.1151	: ada94b0	700	044
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\t^*, 0, ba3e708, 0, 0, 0) Return : ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e6bc, 0, 0, 0) Return: a	732	844
Call Filesystem API	da94b0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^*, 0, ba3e6bc, 0, 0, 0) Return: a	732	844
	da94b0		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3e5c4, 0, 0, 0) R eturn: 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) R eturn: 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) R eturn: 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: a da94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e6bc, 0, 0, 0) Return: ada	732	844
Call Filesystem API	94b0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada	732	844
	9460		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e708, 0, 0, 0) Return: ada 94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e6bc, 0, 0, 0) Return: ada94 b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e6bc, 0, 0, 0) Return: ada94 b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e708, 0, 0, 0) Return: ada94	732	844
Call Filesystem API	b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v0, 0, ba3e6bc, 0, 0, 0) Return: ad	732	844
Call Filesystem API	a94b0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v0, 0, ba3e6bc, 0, 0, 0) Return: ad	732	844
	a94b0		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\t^*, 0, ba3e708, 0, 0, 0) Return: ad a94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc\t^*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc\t^*, 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%lsystem32\WindowsPowerShelllv1.0\Modules\NetLbfo*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetLbfo*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Net\Nat 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Net\Nat 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Net\Nat 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e506, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity\f, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindPristPileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\WindowsPowerShe	732	844
Call Filesystem API	API Name: FindPristPileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSwitchTeam*, 0, ba3er0e, 0, 0, 0) Return: ada94b0 API Name: FindPristPileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSwitchTeam*, 0, ba3er0e, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShelliv1.0\Modules\NetSwitchTeam*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSwitchTeam*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindPristPileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSwitchTeam*, 0, ba3e0bc, 0, 0, 0) Return: ada94b0 API Name: FindPristPileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSwitchTeam*, 0, ba3e708, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: ("windir%isystem32\WindowsPowerShelliv1.0\WindowsPowerShe	732	844
Call Filesystem API	API Name: FindPristPileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetTCPIP 0, ba3e6bc, 0, 0, 0) Return: ada94b0 API Name: FindPristPileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetTCPIP*, 0, ba3e6bc, 0, 0, 0) Return: ada94b0	732	844
Call Filesystem API	API Name: FindPristPileExW Args: (%windir%lassemblyNativeImages_v4.0.30319_32\System.Runteb92aa12#\n^*, 0, ba3b030, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API Call Filesystem API	API Name: FindHirstFileExxW Args: (%windir%\assembly\nativeimages_v4.0.30319_32\system.Runteb92aa12#\cdot 0, ba3b030, 0, 0, 0) Return: ada9df0 API Name: FindHirstFileExxW Args: (7ca66e8, b92e544) Return: 1	2768	2220
		732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules*, 0, ba3e144, 0, 0, 0) Return: ada9df0 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules*, 0, ba3e144, 0, 0, 0) Return: ada9df0	732	
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules*, 0, ba3e144, 0, 0, 0) Return: ada9df0		844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0\footnote{, 0, ba3df54, 0, 0, 0 } Return: ada9df 0	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		
	£ 12-100,00.200.1024		

Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3df54, 0, 0, 0) Return: ada9eb 0	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: ada9df	732	844
Call Filedystem 7 a 1	0	702	
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 T	2768	2220
Call Filesystem API	ype: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\(^1\), 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindristrileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Write File	Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex 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%MicrosoftWindowsiPowerShell/CommandAnalysis/PowerShell_Analysis/CacheEntry_669a0508-00c3-4800-9213-27c8493a9576	2768	2220
	Type: VSDT_COM_DOS	2.00	2223
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)%\WindowsPowerShellModules\PowerShellGet\t^*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShell\Get\t^*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShell\Get\t^*, 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%lsystem32\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%lsystem32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e04c, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\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\BitsTransfen*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\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\BitsTransfen*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\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\t^*, 0, ba3e04c, 0, 0, 0) Return: a da9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, ba3e04c, 0, 0, 0) Return: a da9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e098, 0, 0, 0) Return: a da9df0	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\t^*, 0, ba3e04c, 0, 0, 0) Return: ada9df 0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e04c, 0, 0, 0) Return: ada9df 0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e098, 0, 0, 0) Return: ada9df 0	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\\SCS*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
		732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, ba3e04c, 0, 0, 0) Return: ada9df0		
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\lSE\t^, 0, ba3e04c, 0, 0, 0) Return: ada9df0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\lSE\t^, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
		732 732	844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\lSE\t^, 0, ba3e098, 0, 0, 0) Return: ada9df0		
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, ba3e098, 0, 0, 0) Return: ada9df0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, ba3e098, 0, 0, 0) Return: ada9df0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds*, 0, ba3e04c, 0, 0, 0) Return: ada9df0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\Kds*, 0, ba3e04c, 0, 0, 0) Return: ada9eb0	732 732	844 844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e04c, 0, 0, 0) Return: ada	732	844
Call Filesystem API	9f70 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell\Archive\en-US*, 0, ba3df54, 0, 0, 0) Return the control of	732	844
Call Filesystem API	n: ada9df0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3df54, 0, 0, 0) Retur	732	844
Call Filesystem API	n: ada9df0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3dfa0, 0, 0, 0) Retur	732	844
Call Filesystem API	n: ada9df0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e098, 0, 0, 0) Return: ada	732	844
Call Filesystem API	9df0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e04c, 0, 0, 0) Return:	732	844
Call Filesystem API	ada9df0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e04c, 0, 0, 0) Return:	732	844
Call Filesystem API	ada9df0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e098, 0, 0, 0) Return:	732	844
Call Filesystem API	ada9df0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\v0, 0, ba3e04c, 0, 0, 0) Return: ada9df	732	844
Call Filesystem API	0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\v1, 0, ba3e04c, 0, 0, 0) Return: ada9f7	732	844
Call Filesystem API	0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\v1, 0, ba3e098, 0, 0, 0) Return: ada9df	732	844
·	0		
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\t^, 0, ba3e04c, 0, 0, 0) Return: a da9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e04c, 0, 0, 0) Return: a da9eb0	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) R eturn: 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) R eturn: 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) R eturn: 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: a da9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: ada 9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: ada 9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e098, 0, 0, 0) Return: ada 9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e04c, 0, 0, 0) Return: ada9df 0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e04c, 0, 0, 0) Return: ada9df 0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e098, 0, 0, 0) Return: ada9df 0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v, 0, ba3e04c, 0, 0, 0) Return: ad a9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e04c, 0, 0, 0) Return: ad a9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v0, 0, ba3e098, 0, 0, 0) Return: ad	732	844
Call Filesystem API	a9df0 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%lsystem32\WindowsPowerShelllv1.0\Modules\NetConnection*, 0, ba3e098, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\t^*, 0, ba3e04c, 0, 0, 0) Return: ada9df0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\t^*, 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%lsystem32\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%lsystem32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: ada9df0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetNat\v1, 0, ba3e098, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\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
	ADI Name: FindFirstFilaFyW Arre: (%windir%system30\MindousePowerShall) 4 0\MaddalAldtooal\$ 0 hagacon 0 0 0 Data	732	844
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, ba3e098, 0, 0, 0) Return: ada9df0 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\% system 32 \ Windows Power Shell \ V1.0 \ Modules\ Net Switch Team \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	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		732	844
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, ba3e04c, 0, 0, 0) Return: ada9df0		
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: ada9df 0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: ada9df 0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: ada9df 0	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%lsystem32\WindowsPowerShelllv1.0\Modules\NetworkTransition\t^*, 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	$API\ Name: FindFirstFileExW\ Args: (\ wwindir\%lsystem 32 \ Windows Power Shelll \ v1.0 \ Modules \ PKI\ V^*, 0, ba 3e04c, 0, 0, 0)\ Return: ada9df0$	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
	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\PrpDevice*, 0, ba3e04c, 0, 0, 0) Return: ada9eb0		844
Call Filesystem API		732	
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\t^*, 0, ba3e04c, 0, 0, 0) Return: ada9eb0	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\PrintManagement\(^1, 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: ada	732	844
•	9df0		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e04c, 0, 0, 0) Return: ada	732	844
	9df0		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e098, 0, 0, 0) Return: ada	732	844
	9df0		
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: (\ wwindir\% lassembly lNative lmages_v4.0.30319_32 \ lsystem. Core \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration\t^*, 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\Nativelmages_v4.0.30319_32\System.Runteb92aa12#*, 0, ba38c58, 0, 0, 0) Return: adf7788	732	844
Call Filedystell Al F	All Traine. Filler itself incentifying and incentifying an analysis of the control of the contro	702	044
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.Net\assembly\GAC_MSIL\Microsoft.Windows.Appx.PackageManager.Commands*, 0, ba3b2fc, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,	732	844
	0) Return: adf7548		
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 T	732	844
	ype: VSDT_COM_DOS		
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\t^*, 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)%\WindowsPowerShellModules\PackageManagement\1.0.0.0*, 0, ba3df54, 0, 0, 0) Return: adf738 8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3df54, 0, 0, 0) Return: adf710	732	844
		132	044
can i nosystem ru 1	8		
·		732	
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3dfa0, 0, 0, 0) Return: adf764 8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3dfa0, 0, 0, 0) Return: adf764 8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3dfa0, 0, 0, 0) Return: adf764 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0\tau^*, 0, ba3dfa0, 0, 0, 0) Return: adf764 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\tau^*, 0, ba3e098, 0, 0, 0) Return: adf71c8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\tau^*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732 732	844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3dfa0, 0, 0, 0) Return: adf764 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: adf71c8	732 732 732	844 844 844
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0\tau^*, 0, ba3dfa0, 0, 0, 0) Return: adf764 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\tau^*, 0, ba3e098, 0, 0, 0) Return: adf71c8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\tau^*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732 732	844 844
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0\tau^*, 0, ba3dfa0, 0, 0, 0) Return: adf764 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\tau^*, 0, ba3e098, 0, 0, 0) Return: adf71c8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\tau^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\tau^*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732 732 732	844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0\tau^*, 0, ba3dfa0, 0, 0, 0) Return: adf764 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\tau^*, 0, ba3e098, 0, 0, 0) Return: adf71c8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\tau^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\tau^*, 0, ba3e04c, 0, 0, 0) Return: adf7208 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\tau^*, 0, ba3df54, 0, 0, 0) Return: adf7388	732 732 732 732	844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3dfa0, 0, 0, 0) Return: adf764 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: adf71c8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e04c, 0, 0, 0) Return: adf7208 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 3.5*, 0, ba3df54, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 3.5*, 0, ba3df54, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 3.5*, 0, ba3df30, 0, 0, 0) Return: adf7108	732 732 732 732 732 732	844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, ba3dfa0, 0, 0, 0) Return: adf764 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: adf71c8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e04c, 0, 0, 0) Return: adf7208 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3df54, 0, 0, 0) Return: adf7388 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3df54, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3df30, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, ba3e098, 0, 0, 0) Return: adf7108	732 732 732 732 732 732 732	844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0\text{\circ}*, 0, ba3dfa0, 0, 0, 0) Return: adf764 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\text{\circ}*, 0, ba3e098, 0, 0, 0) Return: adf71c8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3e04c, 0, 0, 0) Return: adf7208 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3df54, 0, 0, 0) Return: adf7388 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3df54, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3e098, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3e098, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3e098, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0\text{\color=1}, 0, ba3dfa0, 0, 0, 0) Return: adf764 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1, 0, ba3e098, 0, 0, 0) Return: adf71c8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\1, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\1, 0, ba3e04c, 0, 0, 0) Return: adf7208 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\1, 3.3.5\1, 0, ba3df54, 0, 0, 0) Return: adf7388 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\1, 3.3.5\1, 0, ba3df54, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\1, 0, ba3e098, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\1, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellModules\PowerShellGet\1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellModules\PowerShellGet\1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellModules\PowerShellGet\1, 0, ba3e04c, 0, 0, 0) Return: adf7108	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0\text{\circ}*, 0, ba3dfa0, 0, 0, 0) Return: adf764 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\text{\circ}*, 0, ba3e098, 0, 0, 0) Return: adf71c8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3e04c, 0, 0, 0) Return: adf7208 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3df54, 0, 0, 0) Return: adf7388 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3df54, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3e098, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3e098, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3e098, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\text{\circ}*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844

-			
Call Filesystem AD!	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e04c, 0, 0, 0) Return: adf71c8	732	844
	API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, ba3e098, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, ba3e098, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\BitsTransfert*, 0, ba3e098, 0, 0, 0) Return: adf7208	732	844
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
-			
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e04c, 0, 0, 0) Return: a	732	844
-	df7408	702	
-	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e04c, 0, 0, 0) Return: a	732	844
	df7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e098, 0, 0, 0) Return: a	732	844
	df7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\Dism*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
-			
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\\VindowsPowerShell\v1.0\\Modules\DnsClient\t^*, 0, ba3e098, 0, 0, 0) Return: adf7148	732	844
	API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e04c, 0, 0, 0) Return: adf710	732	844
8		702	
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e04c, 0, 0, 0) Return: adf764 8	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%lsystem32!WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, ba3e098, 0, 0, 0) Return: adf714 8	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
-	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e098, 0, 0, 0) Return: adf7388	732	844
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e04c, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\lSE*, 0, ba3e098, 0, 0, 0) Return: adf7388	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e04c, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, ba3e098, 0, 0, 0) Return: adf7648	732	844
-	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\t^, 0, ba3e04c, 0, 0, 0) Return: adf7 408	732	844
-	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e04c, 0, 0, 0) Return: adf7 208	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3df54, 0, 0, 0) Returns	732	844
	n: adf7388 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3df54, 0, 0, 0) Retur	732	844
n	n: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, ba3dfa0, 0, 0, 0) Retur	732	844
n	n: adf7108		
1	API Name: FindFirstFileExW Args: (%windir%lsystem32;WindowsPowerShell\v1.0!Modules\Microsoft.PowerShell.Archive\t^*, 0, ba3e098, 0, 0, 0) Return: adf7 108	732	844
a	API Name: FindFirstFileExW Args: (%windir%lsystem32!WindowsPowerShell\v1.0!Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%lsystem32;WindowsPowerShellIv1.0;Modules\Microsoft.PowerShell.Diagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
a	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^, 0, ba3e098, 0, 0, 0) Return:	732	844
Call Filesystem API A	adf7108		
Call Filesystem API A Call Filesystem API A 8 8	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf710 8	732	844
Call Filesystem API A Call Filesystem API A Call Filesystem API A 8 8	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf710 8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf738	732 732	844
Call Filesystem API A Call Filesystem API A 8 8 Call Filesystem API A 8 8	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf710 8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf738 8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e098, 0, 0, 0) Return: adf710		
Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf710 8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf738 8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e098, 0, 0, 0) Return: adf710	732 732	844 844 844
Call Filesystem API A Call Filesystem API A	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf710 8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf738 8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e098, 0, 0, 0) Return: adf710 8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e04c, 0, 0, 0) Return	732 732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e04c, 0, 0, 0) Return: a	732	844
Call Filesystem API	df7288 ADI Namo: FindFindFileSVM Assoc / 9/ vindsis9/ Souther 20/Windows Power Shall of Medida Missoc of Flourer Shall Operation 10 to 20/44 0 0 0 0 Detugs a	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^, 0, ba3e04c, 0, 0, 0) Return: a df71c8	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) R eturn: 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) R	732	844
Call Filesystem API	eturn: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\V1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3dfa0, 0, 0, 0, 0) R	732	844
Call Filacustom ADI	eturn: ad/7648 ADI Namo: FindEilot-VM Asso: / 9/ windfin/ Invators 20/Windows Payer-Phalliud (Medulac) Misson of Payer-Phall Operal Hilat 0, ho2e009, 0, 0, 0,). Payers of	799	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.0DataUtils\t^*, 0, ba3e098, 0, 0, 0) Return: a df7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: adf 7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\t^*, 0, ba3e04c, 0, 0, 0) Return: adf 7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e098, 0, 0, 0) Return: adf 7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e04c, 0, 0, 0) Return: adf710 8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e04c, 0, 0, 0) Return: adf764	732	844
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e098, 0, 0, 0, 0) Return: adf710	732	844
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v1.0, ba3e04c, 0, 0, 0) Return: ad	732	844
Call Filesystem API	17108		844
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\t^*, 0, ba3e04c, 0, 0, 0) Return: ad f7388	732	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e098, 0, 0, 0) Return: ad 17108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\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		732	844
	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetEventPacketCapture*, 0, ba3e04c, 0, 0, 0) Return: adf7388		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\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\WindowsPowerShelllv1.0\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%lsystem32\WindowsPowerShelllv1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf71c8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\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: add7208	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\WindowsPowerShelliv1.0lModules\NetSwitchTeam*, 0, ba3e096, 0, 0, 0) Return: adi7388	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetTCPIP*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetTCPIP*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0lModules\NetTCPIP*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API	ADI Name: FindFiretFileFy/M Area: / 9/ windir9/ austom20/Mindow20/		844
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf710 8	732	
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf718	732	844
Call Filesystem API Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf718 8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: adf710		844
	8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf718 8	732	
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf718 8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: adf710 8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Call Filesystem API Call Filesystem API Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf718 8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: adf710 8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732 732 732 732	844 844
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf718 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: adf710 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7388 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetworkTransition*, 0, ba3e098, 0, 0, 0) Return: adf7108	732 732 732 732 732 732	844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf718 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: adf710 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7388 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e098, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732 732 732 732 732 732 732	844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\t^*, 0, ba3e04c, 0, 0, 0) Return: adf718 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\t^*, 0, ba3e098, 0, 0, 0) Return: adf710 BAPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition\t^*, 0, ba3e098, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7488	732 732 732 732 732 732 732 732	844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\t^*, 0, ba3e04c, 0, 0, 0) Return: adf718 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\t^*, 0, ba3e098, 0, 0, 0) Return: adf710 BAPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\\t^*, 0, ba3e098, 0, 0, 0) 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\\t^*, 0, ba3e098, 0, 0, 0) 0) Return: adf7648	732 732 732 732 732 732 732 732 732	844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf718 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: adf710 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e098, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\N*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\N*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\N*, 0, ba3e098, 0, 0, 0) Return: adf7648 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PR\N*, 0, ba3e098, 0, 0, 0) Return: adf7288	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf718 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: adf710 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e098, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\l*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\l*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\l*, 0, ba3e04c, 0, 0, 0) Return: adf7648 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PR\l*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PR\l*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrDevice*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrDevice*, 0, ba3e04c, 0, 0, 0) Return: adf7168	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf718 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: adf710 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e098, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\N*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\N*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\N*, 0, ba3e098, 0, 0, 0) Return: adf7648 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PR\N*, 0, ba3e098, 0, 0, 0) Return: adf7288	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e04c, 0, 0, 0) Return: adf718 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: adf710 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e098, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\l*, 0, ba3e04c, 0, 0, 0) Return: adf7108 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\l*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\l*, 0, ba3e04c, 0, 0, 0) Return: adf7648 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PR\l*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PR\l*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrDevice*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrDevice*, 0, ba3e04c, 0, 0, 0) Return: adf7168	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844

Set Section Set Section Se				
Company	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, ba3e098, 0, 0, 0) Return: adf7648	732	844
Temperate	Call Filesystem API		732	844
Miles	Call Filesystem API		732	844
Miles Mile	Call Filesystem API		732	844
Million Mill	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\IModules\PSDiagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Milliagenerials	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Add 1997 Add	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
Add 1997 Add	Call Filesystem API	API Name: FindFirstFileExW Aras: (%windir%system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, ba3e04c, 0, 0, 0) Return; adf7188	732	844
Add Section Statistical Content Add Section Emitted and years (section) Add Section (1985) Add Section (19				844
March Property P				
Professionaria Prof				
Personant Pers				***
March Marc				
Column				
Add				
All Proposed Prince All Pr				
March Although A	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, ba3e098, 0, 0, 0) Return: adf7108	732	844
March All Part Pa	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\tau, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Mail March March March March March Mail Ma	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\footnote{, 0, ba3e04c, 0, 0, 0 } Return: adf7108	732	844
AFF Targeton AP	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, ba3e098, 0, 0, 0) Return: adf7148	732	844
All Finderpoint AFT	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ system 32 \ Windows PowerShell \ v1.0 \ Modules\ TLSI^*,\ 0,\ ba3e04c,\ 0,\ 0,\ 0)\ Return:\ adf7108$	732	844
All Name Profit or Septimen AS All Name Profit or Septimen AS 20 20 20 20 20 20 20 2	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
March September AF Aff Name Front Profit Policy May 1, Name Front Profit Policy Name Front Profit Policy Name Front Profit Policy (1) Name Front Profit Policy (1) Name Front Profit Policy (1) Name Front Profit Policy Name Front Profit Polic	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, ba3e098, 0, 0, 0) Return: adf7148	732	844
Control Control And Name President Service Ser	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Control Control And Name President Service Ser				844
APT March President Age Section Sect				
64 Flagogram AR AR Name in Professional Ways ("school/hogopart/2004/color/bloopa				
APT Name First Part Willing APT Name First Part Will By (2) (Vision Strophen COVINCIAN Discoult Process of Nacholace (0, 10) Patern will 700 72 84				
Old Telegram APT	•			
APT Secretar APT APT APT APT Control of September 1 APT				
Cell Flaupsinn APR				
Cell Picuyatan APP				***
Call Fleegolan AP API Name FindFindField Magar (% sheaft hipspend/20/Modes/PeedSelvi 1 (30Modes/PeedSelvi 1, 0 babbles, 0, 0 0) Februm add7163 722 844				
Call Filesystem APT	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, ba3e04c, 0, 0, 0) Return: adf7648	732	844
Call Fisiophiam APF	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, ba3e04c, 0, 0, 0) Return: adf71c8	732	844
Call Fileopstein APT	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, ba3e098, 0, 0, 0) Return: adf7648	732	844
Call Fleeystem API	Call Filesystem API		732	844
B Call Fleogration API	Call Filesystem API		732	844
Call Fleeystem AP AP Name: FindFineEvit Args: (%windrikisystem32WindowsPowerShell tr.DModules/WindowsErroReporting**, 0, ba3604c, 0, 0, 0) Return: adf7288 732 844 Call Fleeystem AP AP Name: FindFineEvit Args: (%windrikisystem32WindowsPowerShell tr.DModules/WindowsErroReporting**, 0, ba3604c, 0, 0, 0) Return: adf7288 732 844 Call Fleeystem AP AP Name: FindFineEvit Args: (%windrikisystem32WindowsPowerShell** tr.DModules/WindowsEpdate**, 0, ba3604c, 0, 0, 0) Return: adf7288 732 844 Call Fleeystem AP AP Name: FindFineEvit Args: (%windrikisystem32WindowsPowerShell** tr.DModules/WindowsEpdate**, 0, ba3604c, 0, 0, 0) Return: adf7488 732 844 Call Fleeystem AP AP Name: FindFineEvit Args: (%windrikisystem32WindowsPowerShell** tr.DModules/WindowsEpdate**, 0, ba3604c, 0, 0, 0) Return: adf7488 732 844 Call Fleeystem AP AP Name: FindFineEvit Args: (%windrikisystem32WindowsPowerShell** tr.DModules*WindowsEpdate**), 0, ba3604c, 0, 0, 0) Return: adf7488 732 844 Call Fleeystem AP AP Name: FindFineEvit Args: (%windrikisystem32WindowsPowerShell** tr.DModules*WindowsEpdate**), 0, ba3606c, 0, 0, 0) Return: adf7488 732 844 Call Fleeystem AP AP Name: FindFineEvit Args: (%windrikisystem32WindowsPowerShell** tr.DModules**), 0, ba36180, 0, 0, 0) Return: adf7488 732 844 Call Fleeystem AP AP Name: FindFineEvit Args: (%ProgramFineEvit Args)seCatheEntry, 88806b05766-4615742-04886846417 732 844 Call Fleeystem AP AP Name: FindFineEvit Args: (%ProgramFineEvit Args)seCatheEntry, 88806b05766-4615742-0488866417 732 844 Call Fleeystem AP AP Name: FindFineEvit Args: (%ProgramFineEvit Args)seCatheEntry, 88806b05766-4615742-04888646417 732 844 Call Fleeystem AP AP Name: FindFineEvit Args: (%ProgramFineEvit Args)seCatheEntry, 88806b05766-4615742-04888646417 732 844 Call Fleeystem AP AP Name: FindFineEvit Args: (%ProgramFineEvit Args)seCatheEntry, 0, 0, 0) Return: adf7188 732 844 Call Fleeystem AP AP Name: FindFineEvit Args: (%ProgramFineEvit Args)seCatheShoules*PackageManagement 1.0.00**, 0, 0, 0	Call Filesystem API		732	844
Call Filesystem AP API Name: FindFirstFileEW Arg: ("windfrishgestem22WindowsPowerShelfv1 OModules/WindowsEprorReporting")", ba36088, 0, 0, 0) Return: adf7288 732 844	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem AP API Name: FindFirstFileStW Args: (%winds*)system2XWindowsPowerShell* / OxfootidestWindowsUpdate**, 0, basicable*, 0, 0, 0) Return: add71288 732 844 Call Filesystem API API Name: FindFirstFileStW Args: (%winds*)system32WindowsPowerShell* / OxfootidestWindowsUpdate**, 0, basicable**, 0, basi	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: FindFirsFileExW Age; (%windfif/sipystem2)WindowsPowerShell/t 10ModulesWindowsUpdater*, 0, ba3e04e, 0, 0, 0) Return: adf7108 732 844 Call Filesystem API API Name: FindFirsFileExW Age; (%windfif/sipystem32WindowsPowerShell/t 10ModulesWindowsUpdater*, 0, ba3e04e, 0, 0, 0) Return: adf7488 732 844 Call Filesystem API API Name: FindFirsFileExW Age; (%windfif/sipystem32WindowsPowerShell/t 10Modules)*, 0, ba3e16e, 0, 0, 0, 0 Return: adf7488 732 844 Wrife File Path: %LOCALAPPDATA;MilkCrosoftWindowsPowerShellCommandAnalysis PowerShell AnalysisCacheEntry_68(060-05766-4c81-6742-04(8)8846c4 Ty) 2768 2220 Call Filesystem API API Name: FindNesfileW Age; (*7z26938, 826244) Return: 1 2768 2220 Wrife File Path: %LOCALAPPDATA;MilkCrosoftWindowsPowerShell AnalysisCacheEntry_68(060-05766-4c81-6742-04(8)8846c4 Ty) 732 844 Wrife File Path: %LOCALAPPDATA;MilkCrosoftWindowsPowerShellModules**, 0, ba3e144, 0, 0, 0) Return: adf7168 732 844 Call Filesystem API API Name: FindFirsFileExW Age; (%ProgramFiles;68)%WindowsPowerShellModules**, 0, ba3e144, 0, 0, 0) Return: adf7168 732 844 Call Filesystem API API Name: FindFirsFileExW Age; (%ProgramFiles;68)%WindowsPowerShellModules**, 0, ba3e144, 0, 0, 0) Return: adf7168 732 844 <	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\% lsystem 32 \ Windows Power Shell \ v1.0 \ Modules \ Windows Error Reporting \ v3.0, ba3e098, 0, 0, 0)\ Return: adf 7648$	732	844
Call Filesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\\Modules\\WindowsUpdate*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
API Name: FindFirstFileExW Args: (%windin%system32WindowsPowerShellV.0Modules*), 0, ta36+150, 0, 0, 0) Return: ad77408	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\\Modules\\WindowsUpdate*, 0, ba3e04c, 0, 0, 0) Return: adf7108	732	844
Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShellCommandAnalysisiPowerShell AnalysisCacheEntry_68fd06b0-5766-4c81-6742-04f8b8d4fc4 Ty pe: VSDT_COM_DOS 2768 2220	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, ba3e098, 0, 0, 0) Return: adf7488	732	844
Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShellCommandAnalysisiPowerShell AnalysisCacheEntry_68fd06b0-5766-4c81-6742-04f8b8d4fc4 Ty pe: VSDT_COM_DOS 2768 2220	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, ba3e190, 0, 0, 0) Return: adf7408	732	844
Cal Fleeystem API API Name: FindNextFileW Args: (7d2b938, b92e544) Return: 1 2768 2220 Write File Path: %LOCALAPPDATA%:MicrosoftWindowsPowerShell/CommandAnalysis/PowerShell_Analysis/CachelEntry_68f066b0-5766-4c81-b742-04f8fb8d4fc4 Type: VSDT_COM_DOS 732 844 Write File Path: %LOCALAPPDATA%:MicrosoftWindowsPowerShell/CommandAnalysis/PowerShell_Analysis/CachelEntry_68f06b0-5766-4c81-b742-04f8fb8d4fc4 Type: VSDT_COM_DOS 732 844 Cal Fleeystem API API Name: FindFireifireiExW Args: (%ProgramFiles(x68)%:WindowsPowerShellModulest*, 0, ba3e144, 0, 0, 0) Return: addf7188 732 844 Cal Fleeystem API API Name: FindFireiFileExW Args: (%ProgramFiles(x68)%:WindowsPowerShellModulest*, 0, ba3e144, 0, 0, 0) Return: addf7188 732 844 Cal Fleeystem API API Name: FindFireiFileExW Args: (%ProgramFiles(x68)%:WindowsPowerShellModulestPackageManagement*, 0, ba3e04c, 0, 0, 0) Return: addf7188 732 844 Cal Fleeystem API API Name: FindFireiFileExW Args: (%ProgramFiles(x68)%:WindowsPowerShellModulestPackageManagement*), 0, ba3e04c, 0, 0, 0) Return: addf7408 732 844 Cal Filesystem API API Name: FindFireiFileExW Args: (%ProgramFiles(x68)%:WindowsPowerShellModulesPackageManagement*), 0, ba3edf54, 0, 0, 0) Return: addf7408 732 844 Cal Filesystem API API Name: FindFireiFileExW Args: (%ProgramFiles(x68)%:WindowsPowerShellModules		Path: %LOCALAPPDATA%IMicrosoftlWindowsIPowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_68fd06b0-5766-4c81-b742-04f8fb8d4fc4 Ty		2220
Path: %LOCALAPPDATA%MicrosoftWindowsPowerShelltCommandAnalysisPowerShell AnalysisCacheEntry_68f066b0-5766-4c81-b742-04f8fb8d4fc4 Ty pe: VSDT_COM_DOS	Write File	Path: %LOCALAPPDATA%IMicrosoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Pe: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindowsiPowerShell*CommandAnalysis/PowerShell*Analysis/CacheIndex Type: VSDT_COM_DOS 732 844	Call Filesystem API	API Name: FindNextFileW Args: (7d2b938, b92e544) Return: 1	2768	2220
Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*, 0, ba3e144, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*, 0, ba3e144, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, 0, ba3edf54, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, 0, ba3edf64, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, 0, ba3edf64, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: Find	Write File		732	844
Call Filesystem API API Name: FindNextFileW Args: (adf7188, ba3e154) Return: 1 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%FrogramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, 0, ba3df54, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, 0, ba3df54, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, 0, ba3dfa0, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, 0, ba3e08e, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, 0, ba3e08e, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%Program	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)%WindowsPowerShellModules)* (0, ba3e144, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, (0, ba3e04c, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, (0, ba3e04c, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*(1.0.0.01*, 0, ba3df54, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*(1.0.0.01*, 0, ba3df54, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*(1.0.0.01*, 0, ba3e098, 0, 0, 0) Return: adf748 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*(*, 0, ba3e098, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*(*, 0, ba3e04c, 0, 0, 0) Return: adf7408 732 844 C	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)%WindowsPowerShellModules)* (0, ba3e144, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, (0, ba3e04c, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*, (0, ba3e04c, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*(1.0.0.01*, 0, ba3df54, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*(1.0.0.01*, 0, ba3df54, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*(1.0.0.01*, 0, ba3e098, 0, 0, 0) Return: adf748 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*(*, 0, ba3e098, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)*PackageManagement*(*, 0, ba3e04c, 0, 0, 0) Return: adf7408 732 844 C				844
Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement 0, ba3e04c, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement 0, ba3e04c, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement 0, ba3e04c, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement 0, 0, 0), 0, ba3df54, 0, 0, 0) Return: adf740 8 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement 0, 0, 0), 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,				844
Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement**, 0, ba3e04c, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement**, 0, ba3df54, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement**, 0, ba3df34, 0, 0, 0) Return: adf740 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement**, 0, ba3e098, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement**, 0, ba3e098, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement**, 0, ba3e04c, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement**, 0, ba3e04c, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement**, 0, ba3e04c, 0, 0, 0) Return: adf7188 732 844				
API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement\1.0.0.0\tag{0}*, 0, ba3df54, 0, 0, 0) Return: adf740 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement\1.0.0.0\tag{0}*, 0, ba3df54, 0, 0, 0) Return: adf740 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement\1.0.0.0\tag{0}*, 0, ba3dfa0, 0, 0, 0) Return: adf740 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement\1.0.0.0\tag{0}*, 0, ba3dfa0, 0, 0, 0) Return: adf740 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement\1.0.0.0\tag{0}*, 0, ba3efa0, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\1*, 0, ba3efa0, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\1*, 0, ba3efa04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\1*, 0, ba3efa04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\1*, 0, ba3efa04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\1*, 0, ba3df54, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\1*, 0, ba3df54, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\1*, 0, ba3df54, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\1*, 0, ba3df54, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\1*, 0, ba3df34, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\1*, 0, ba3df34, 0, 0, 0) Return: adf7188 API Name: FindFirst	,			
8 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement\1.0.0.0*, 0, ba3df54, 0, 0, 0) Return: adf740 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement\1.0.0.0*, 0, ba3dfa0, 0, 0, 0) Return: adf718 8 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester*, 0, ba3e04c, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester*, 0, ba3e04c, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844				
8 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0*, 0, ba3dfa0, 0, 0, 0) Return: adf718 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester*, 0, ba3e04c, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester*, 0, ba3e04c, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844	·	8		
8 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagementt*, 0, ba3e098, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pestert*, 0, ba3e04c, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pestert*, 0, ba3e04c, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pestert3.3.5\forall *, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pestert3.3.5\forall *, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pestert3.3.5\forall *, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844	·	8		
Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pesten*, 0, ba3e04c, 0, 0, 0) Return: adf7408 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pesten*, 0, ba3e04c, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pesten(3.3.5)*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pesten(3.3.5)*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pesten(3.3.5)*, 0, ba3df60, 0, 0, 0) Return: adf7188 732 844			. 52	
Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pesten*, 0, ba3e04c, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pesten\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pesten\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pesten\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\t^*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pesten*, 0, ba3e04c, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pesten\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pesten\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pesten\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pestert*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\3.3.5\\^*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\3.3.5\\^*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\3.3.5\\^*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844				844
Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\Pester\3.3.5*, 0, ba3df54, 0, 0, 0) Return: adf7188 732 844 Call Filesystem API API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\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\3.3.5*, 0, ba3dfa0, 0, 0, 0) Return: adf7188 732 844	•			
	•			
	Call Filesystem API			

Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet\tau, 0, ba3e04c, 0, 0, 0) Return: adf7188		
Call Filesystem API		732	844
	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGet\t^*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules*, 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\BitsTransfen\^, 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 WindowsPowerShelllv1.0lModules\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: a	732	844
•	df7408		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e04c, 0, 0, 0) Return: a	732	844
	df7408		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e098, 0, 0, 0) Return: a	732	844
-	df71c8		
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\t^*, 0, ba3e04c, 0, 0, 0) Return: adf728	732	844
	8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v1, 0, ba3e04c, 0, 0, 0) Return: adf720	732	844
	8		
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%lsystem32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, ba3e098, 0, 0, 0) Return: adf728	732	844
Odii i iiosystem Ai i			
Odii i ilosystom za i	8		
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
•		732 732	844 844
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e098, 0, 0, 0) Return: adf7408	732 732	844 844
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732 732 732	844 844 844
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e098, 0, 0, 0) Return: adf7408	732 732	844 844
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732 732 732	844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\n^*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\n^*, 0, ba3e098, 0, 0, 0) Return: adf7188	732 732 732 732 732	844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732 732 732 732 732 732 732	844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\v*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\v*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732 732 732 732 732 732 732 732	844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732 732 732 732 732 732 732	844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\v*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\v*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732 732 732 732 732 732 732 732	844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\v*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\v*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v*, 0, ba3e096, 0, 0, 0) Return: adf7188	732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IKds\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IKds\v*, 0, ba3e098, 0, 0, 0) Return: adf7188	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name:	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISC\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Idcs\Idcs\Idcs\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Idcs\Idcs\Idcs\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Idcs\Idcs\Idcs\Iv*, 0, ba3e04c, 0, 0, 0) Return: adf7	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\I\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name:	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Arg	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\n^*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\n^*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\n^*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids\n^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%win	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\In*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\In*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\In*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\In*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\In*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\In*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\In*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids\Ind\IndowsPowerShell\v1.0\Modules\Ids\IndowsPowerShell\v1.0\Modules\Ids\IndowsPowerShell\v1.0\Modules\Ids\IndowsPowerShell\v1.0\Modules\Ids\IndowsPowerShell\v1.0\Modules\Ids\IndowsPowerShell\v1.0\Modules\Ids\IndowsPowerShell\v1.0\Modules\Ids\IndowsPowerShell\v1.0\Modules\Ids\IndowsPowerShell\v1.0\Modules\Ids\IndowsPowerShell\v1.0\Modules\Ids\IndowsPowerShell\v1.0\Modules\Ids\IndowsPowerShell\v1.0\Modules\Ids\IndowsPowerShell\v1.0\Modules\IndowsPowerShell\v1.0\Modules\Ind	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\In*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\In*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\In*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\In*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\In*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\In*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\In*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids\In\In*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids\In\In*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids\In\In*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids\In\In*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\International\taukspaces\t	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Ids*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFile	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\International\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\tv1.0\Modules\ISCS\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\tv1.0\Modules\ISCS\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\tv1.0\Modules\ISCS\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\tv1.0\Modules\ISE\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\tv1.0\Modules\ISE\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\tv1.0\Modules\ISE\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\tv1.0\Modules\ISE\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\tv1.0\Modules\Idens\Idens\tau (0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\tv1.0\Modules\Idens\Idens\tau (0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\tv1.0\Modules\Idens\Idens\tau (0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\tv1.0\Modules\Idens\Idens\tau (0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\tv1.0\Modules\Idens\Idens\tau\tex	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\taukstarta (0, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\taukstarta (0, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\taukstarta (0, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\taukstarta (0, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\taukstarta (0, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\taukstarta (0, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\taukstarta (0, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\taukstarta (0, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\taukstarta (0, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\taukstarta (0, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IXds\taukstarta (0, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IXds\taukstarta (0, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IMicrosoft.PowerShell\Archive\taukstarta (0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IMicrosoft.PowerShell\Archive\taukstarta (0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IMicrosoft.PowerShell\Archive\taukstarta (0, 0, 0)	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv1, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv1, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\ISC\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\ISC\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\ISC\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\ISC\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\IMcrosoft.PowerShell\Archive\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\IMcrosoft.PowerShell\Archive\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\IMcrosoft.PowerShell\Archive\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\IMcrosoft.PowerShell\Archive\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\IMcros	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\w1.0\Modules\International\tautority, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\w1.0\Modules\International\tautority, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\w1.0\Modules\International\tautority, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\w1.0\Modules\International\tautority, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\w1.0\Modules\International\tautority, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\w1.0\Modules\International\tautority, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\w1.0\Modules\International\tautority, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\w1.0\Modules\International\tautority, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\w1.0\Modules\International\tautority, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\w1.0\Modules\International\tautority, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\w1.0\Modules\International\tautority, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\w1.0\Modules\International\tautority, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\w1.0\Modules\International\tautority, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\w1.0\Modules\International\tautority, 0, ba3e04c, 0, 0, 0) Retur	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISC\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISC\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISC\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISC\v1, 0\Modules\ISC\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShelliv1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShelliv1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShelliv1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShelliv1.0\Modules\International*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShelliv1.0\Modules\ISCSI*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShelliv1.0\Modules\ISCSI*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShelliv1.0\Modules\ISE\ISCSI*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShelliv1.0\Modules\ISE\ISCSI*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShelliv1.0\Modules\ISE\ISCSI*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShelliv1.0\Modules\IMcircosoft.PowerShell Archive\I*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShelliv1.0\Modules\IMcircosoft.PowerShell Archive\I*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShelliv1.0\Modules\IMcircosoft.PowerShell Archive\I*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\Iv1.0\Modules\IMcircosoft.PowerShell Archive\I*, 0, ba3df54, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\Iv1.0\Modules\IMcircosoft.PowerShell Archive\I*, 0, ba3df54, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system3z\Windows	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%isystem3z\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%isystem3z\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%isystem3z\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%isystem3z\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%isystem3z\WindowsPowerShell\v1.0\Modules\ISCS\V1, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir\%isystem3z\WindowsPowerShell\v1.0\Modules\ISCS\V1, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (\mindir\mind	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0Modules\International\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\International\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\International\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\ISCSI\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\ISCSI\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\ISE\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\ISE\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\ISE\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\ISE\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\ISE\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\IMicrosoft.PowerShellArchive\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\IMicrosoft.PowerShellArchive\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\IMicrosoft.PowerShellArchive\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\IMicrosoft.PowerShellArchive\(^1\), 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPower	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%isystem3z\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%isystem3z\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%isystem3z\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%isystem3z\WindowsPowerShell\v1.0\Modules\International\v1, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%isystem3z\WindowsPowerShell\v1.0\Modules\ISCS\V1, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir\%isystem3z\WindowsPowerShell\v1.0\Modules\ISCS\V1, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (\mindir\mind	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\International\(^n\), 0 ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\International\(^n\), 0 ba3e04s, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\International\(^n\), 0 ba3e04s, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\International\(^n\), 0 ba3e04s, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\(^n\), 0 ba3e04s, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\(^n\), 0 ba3e04s, 0, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\(^n\), 0 ba3e04s, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\(^n\), 0 ba3e04s, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\(^n\), 0 ba3e04s, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\(^n\), 0 ba3e04s, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\(^n\), 0 ba3e04s, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\(^n\), 0 ba3e04s, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\(^n\), 0 ba3e04s, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\(^n\), 0 ba3e04s, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\(^n\), 0 ba3e04s, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\(^n\), 0 ba3e04s, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\(^n\), 0	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\International\tau{1}, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\International\tau{1}, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\International\tau{1}, 0, ba3e08c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\ISCSI\tau{1}, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\ISCSI\tau{1}, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\ISCSI\tau{1}, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\ISE\tau{1}, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\ISE\tau{1}, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\ISE\tau{1}, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\ISE\tau{1}, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\ISE\tau{1}, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\ISE\tau{1}, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\IMicrosoft.PowerShell.Archive\tau{1}, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\IMicrosoft.PowerShell.Archive\tau{1}, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\IMicrosoft.Po	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelflv1,0Modules\Internationalt*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelflv1,0Modules\Internationalt*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelflv1,0Modules\Internationalt*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelflv1,0Modules\Internationalt*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelflv1,0Modules\Internationalt*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelflv1,0Modules\Internationalt*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelflv1,0Modules\Internationalt*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelflv1,0Modules\Internationalth*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelflv1,0Modules\Internationalth*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelflv1,0Modules\Internationalth*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelflv1,0Modules\Internationalth*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelflv1,0Modules\Internationalth*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelflv1,0Modules\Internationalth*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelflv1,0Modules\Internationalth*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelflv1,0Modules\Internationalth*, 0, ba3e04c, 0, 0, 0) R	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windtr%lsystem32WindowsPowerShelliv1.0Modules\lnternational\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (%windtr%lsystem32WindowsPowerShelliv1.0Modules\lnternational\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (\) \(732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\International\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\International\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\International\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\International\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\International\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\International\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\International\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\International\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\International\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\International\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\International\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\Internations\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShelliv1.0Modules\Internations\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (\swindir\system32\WindowsPowerShelliv1.0Modules\Internations\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (\swindir\system32\WindowsPowerShelliv1.0Modules\Interna	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windtr%lsystem32WindowsPowerShelliv1.0Modules\lnternational\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (%windtr%lsystem32WindowsPowerShelliv1.0Modules\lnternational\)*, 0, ba3e04c, 0, 0, 0 \ Return: adt7188 API Name: FindFirstFileExW Args: (\) \(732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\text{\color=0}, 0, ba3e04c, 0, 0, 0) Return	732	844
Call Filesystem API	: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\v1.0, ba3e098, 0, 0, 0) Return	732	844
Call Filesystem All F	: adf7188	102	044
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^*, 0, ba3e04c, 0, 0, 0) Return: a	732	844
Call Filesustana ADI	df7188	700	044
Call Filesystem API	API Name: FindFirstFileExtW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^*, 0, ba3e04c, 0, 0, 0) Return: a df7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\t^*, 0, ba3df54, 0, 0, 0) R	732	844
	eturn: adf7188		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3df54, 0, 0, 0) R eturn: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3dfa0, 0, 0, 0) R	732	844
	eturn: adf7188		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, ba3e098, 0, 0, 0) Return: a df7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: adf	732	844
	7208		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: adf 7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e098, 0, 0, 0) Return: adf	732	844
	7188		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\t^*, 0, ba3e04c, 0, 0, 0) Return: adf718	732	844
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\t^*, 0, ba3e04c, 0, 0, 0) Return: adf71c	732	844
San i nosystom ruʻl	API Name: Finderirstr-lieExiv Args: (%windir%isystem52/vvindowsPowerSneinV1.0/imodulestimicrosoft.PowerSneil.0tility/ , 0, baseu4c, 0, 0, 0) Return: adr/ 1c 8	. 02	V++
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e098, 0, 0, 0, 0) Return: adf748	732	844
Call Eileanntara AE'	8	720	044
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e04c, 0, 0, 0) Return: ad f7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\t^*, 0, ba3e04c, 0, 0, 0) Return: ad	732	844
	f7408		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v1, 0, ba3e098, 0, 0, 0) Return: ad f7188	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%lsystem32\WindowsPowerShelllv1.0\Modules\MsDtc*, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetAdapter*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\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%lsystem32\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%lsystem32\WindowsPowerShelllv1.0\Modules\NetEventPacketCapture*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetEventPacketCapture*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
•			844
Call Filesystem API	API Name: FindFirstFileExtW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, ba3e038, 0, 0, 0) Return: adf7188	732	
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\t^*, 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\v1, 0, ba3e098, 0, 0, 0) Return: adf7408	732	844
Call Filesystem API	API Name: FindFirstFileEx/W 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%lsystem32\WindowsPowerShelllv1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7208	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%lsystem32\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\t^*, 0, ba3e098, 0, 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%lsystem32\WindowsPowerShelllv1.0\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: adf718	732	844
	8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\t^*, 0, ba3e04c, 0, 0, 0) Return: adf718 8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, ba3e098, 0, 0, 0) Return: adf718	732	844
Gail i licayatorii Fu'l	API Name: FinderirstFileExiv Args: (%windir%isystem52/vvindowsPowerSneinV1.0iiwodulestivetworkConnectivityStatus**, 0, ba3e036, 0, 0, 0) Return: adi7 to 8	.02	J
		732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7188		
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
		732 732	844
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732 732	844 844
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition\t^*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732 732 732	844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition\t^*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\\t^*, 0, ba3e098, 0, 0, 0) Return: adf7188	732 732 732 732	844 844 844
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition\t^*, 0, ba3e098, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408	732 732 732	844 844 844

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%lsystem32\WindowsPowerShelllv1.0\Modules\PrintManagement\tau^*, 0, ba3e098, 0, 0, 0) Return: adf7188	732	844
			844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e04c, 0, 0, 0) Return: adf7 288	732	044
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e04c, 0, 0, 0) Return: adf7	732	844
•	208		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e098, 0, 0, 0) Return: adf7	732	844
	408		
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
			844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	
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%lsystem32\WindowsPowerShelllv1.0\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, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileEx:W Args: (%windir%lsystem32\WindowsPowerShelllv1.0\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%lsystem32\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
·	ADI News CindCintCileCVM Area (9 uindig/)		944
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: FindFirstFileEx/W 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%lsystem32\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\t^*, 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: FindFirstFileEx:W Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Wdac\t^, 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: adf740	732	844
	8		
Call Filesystem API	API Name: FindFirstFileEx:W Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense\t^*, 0, ba3e04c, 0, 0, 0) Return: adf718	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, ba3e098, 0, 0, 0) Return: adf718 8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7188	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\t^*, 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) R	732	844
W 2 E1	eturn: adf71c8	0700	0000
Write File	Path: %LOCALAPPDATA%IMicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9e171436-c937-4495-97a3-6ab639ad9344 Type: VSDT_COM_DOS	2768	2220
		0700	0000
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
		732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9e171436-c937-4495-97a3-6ab639ad9344		
	Type: VSDT_COM_DOS		
Write File Write File		732	844
	Type: VSDT_COM_DOS	732 732	844 844
Write File	Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS		
Write File Call Filesystem API	Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288	732	844
Write File Call Filesystem API Call Filesystem API Call Filesystem API	Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288	732 732 732	844 844
Write File Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCachelndex Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7488	732 732 732 732	844 844 844
Write File Call Filesystem API Call Filesystem API Call Filesystem API	Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288	732 732 732	844 844 844
Write File Call Filesystem API	Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCachelndex Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3df54, 0, 0, 0) Return: adf728	732 732 732 732 732	844 844 844 844
Write File Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCachelndex Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf728	732 732 732 732	844 844 844
Write File Call Filesystem API	Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCachelndex Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3df54, 0, 0, 0) Return: adf728 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3df54, 0, 0, 0) Return: adf740	732 732 732 732 732 732	844 844 844 844 844
Write File Call Filesystem API	Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCachelndex Type: VSDT_COM_DOS API Name: FindFirstFileEx\W Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileEx\W Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileEx\W Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileEx\W Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileEx\W Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileEx\W Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3df54, 0, 0, 0) Return: adf728 8 API Name: FindFirstFileEx\W Args: (%ProgramFiles(x86)\%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3df54, 0, 0, 0) Return: adf728	732 732 732 732 732	844 844 844 844
Write File Call Filesystem API	Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\\(\text{Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%ProgramFiles(x86)\(\text{\text{Windows\PowerShell\Modules\\^*}\), 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)\(\text{\text{Windows\PowerShell\Modules\\^*}\), 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)\(\text{\text{\text{Windows\PowerShell\Modules\PackageManagement\\^*}\), 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)\(\text{\text{\text{Windows\PowerShell\Modules\PackageManagement\\^*}\), 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)\(\text{\text{\text{Windows\PowerShell\Modules\PackageManagement\\^*}\), 0, ba3df54, 0, 0, 0) Return: adf728 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)\(\text{\text{\text{\text{Windows\PowerShell\Modules\PackageManagement\\^*}\), 0, ba3df54, 0, 0, 0) Return: adf740 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)\(\text{\tex	732 732 732 732 732 732	844 844 844 844 844
Write File Call Filesystem API	Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3df54, 0, 0, 0) Return: adf728 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 1.0.0.0*, 0, ba3df54, 0, 0, 0) Return: adf740 8 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 1.0.0.0*, 0, ba3df54, 0, 0, 0) Return: adf728 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: adf728 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: adf728	732 732 732 732 732 732 732	844 844 844 844 844 844
Write File Call Filesystem API	Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\\(\text{Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCachelndex\ Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%ProgramFiles(x86)\(\text{\text{Windows\PowerShell\Modules\PackageManagement*\), 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)\(\text{\text{\text{Windows\PowerShell\Modules\PackageManagement*\}\), 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)\(\text{\text{\text{Windows\PowerShell\Modules\PackageManagement*\}\), 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (\text{\text{\text{\text{WrogramFiles\(x86\)}\(\text{\text{Windows\PowerShell\Modules\PackageManagement*\}\), 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (\text{\	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844
Write File Call Filesystem API	Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCachelndex Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf728 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3df54, 0, 0, 0) Return: adf740 BAPI Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3df54, 0, 0, 0) Return: adf728 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: adf728 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e098, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844
Write File Call Filesystem API	Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\\(\text{Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCachelndex\ Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%ProgramFiles(x86)\(\text{\text{Windows\PowerShell\Modules\PackageManagement*\), 0, ba3e144, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)\(\text{\text{\text{Windows\PowerShell\Modules\PackageManagement*\}\), 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)\(\text{\text{\text{Windows\PowerShell\Modules\PackageManagement*\}\), 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (\text{\text{\text{\text{WrogramFiles\(x86\)}\(\text{\text{Windows\PowerShell\Modules\PackageManagement*\}\), 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (\text{\	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844

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\t^*, 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\PowerShellGett*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\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\AppLocken**, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLockert*, 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: FindFirstFileEx/W Args: (%windir%lsystem32\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\t^*, 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, 0, ba3e04c, 0, 0, 0) Return: a df7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, ba3e04c, 0, 0, 0) Return: a df7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, ba3e098, 0, 0, 0) Return: a df7288	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\v1.0, ba3e04c, 0, 0, 0) Return: adf728 8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, ba3e04c, 0, 0, 0) Return: adf728 8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, ba3e098, 0, 0, 0) Return: adf728 8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 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: FindristrineExW Aigs. (%windir%lsystem32!WindowsPowerShell\v1.0\Modules\iSCSl\t^, 0, ba3e04c, 0, 0, 0) Return: adi7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\iSCS\\1, 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\\SE*, 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: adf7 408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\t^, 0, ba3e04c, 0, 0, 0) Return: adf7 288	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: adf7 288	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: adf728 8	732	844

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e04c, 0, 0, 0) Return: adf740	732	844
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, ba3e098, 0, 0, 0) Return: adf728	732	844
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, ba3e04c, 0, 0, 0) Return	732	844
Call Filesystem API	: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e04c, 0, 0, 0) Return	732	844
Call Filesystem API	: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, ba3e098, 0, 0, 0) Return	732	844
Call Filesystem API	: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\v1, 0, ba3e04c, 0, 0, 0) Return: a	732	844
Call Filesystem API	df7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell\.ODataUtils\v1, 0, ba3e04c, 0, 0, 0) Return: a	732	844
Call Filesystem API	df7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell\.ODataUtils\en-US\v1, 0, ba3df54, 0, 0, 0) R	732	844
Call Filesystem API	eturn: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell\.ODataUtils\en-US*, 0, ba3df54, 0, 0, 0) R	732	844
	eturn: adf7408		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, ba3dfa0, 0, 0, 0) R eturn: adt/7408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^*, 0, ba3e098, 0, 0, 0) Return: a df7488	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: adf 7288	732	844
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e04c, 0, 0, 0) Return: adf 7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, ba3e098, 0, 0, 0) Return: adf 7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, ba3e04c, 0, 0, 0) Return: adf728 8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\Microsoft.PowerShell.Utility\1*, 0, ba3e04c, 0, 0, 0) Return: adf728 8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShellIv1.0lModules\Microsoft.PowerShell.Utility*, 0, ba3e098, 0, 0, 0) Return: adf728 8	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e04c, 0, 0, 0) Return: ad f7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e04c, 0, 0, 0) Return: ad 17288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, ba3e098, 0, 0, 0) Return: ad 17408	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc\t^*, 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\NetAdapten*, 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%lsystem32\WindowsPowerShelllv1.0\Modules\NetEventPacketCapture\(^*, 0, ba3e04c, 0, 0, 0 \) Return: adf7288	732	844
· ·			
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0lModules\NetEventPacketCapture*, 0, ba3e04c, 0, 0, 0) Return: adf7488	732	844
Call Filesystem API			
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0lModules\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: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732 732	844 844
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, ba3e098, 0, 0, 0) Return: adf7408	732 732 732	844 844 844
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e04c, 0, 0, 0) Return: adf7488	732 732 732 732	844 844 844
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732 732 732 732 732	844 844 844
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e04c, 0, 0, 0) Return: adf7488	732 732 732 732	844 844 844
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732 732 732 732 732	844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNat*, 0, ba3e098, 0, 0, 0) Return: adf7408	732 732 732 732 732 732	844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetLbfo*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetNat*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetQos*, 0, 0, 0, 0) Return: adf7288	732 732 732 732 732 732 732	844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatt*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatt*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatt*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288	732 732 732 732 732 732 732 732	844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo**, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl**, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl**, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetNatl**, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e098, 0, 0, 0) Return: adf7288	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNat**, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNat**, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetNat**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7408	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e098, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7288	732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo**, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 A	732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos*, 0, ba3e098, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindF	732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfo**, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetNatl**, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetQos**, 0, ba3e098, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity**, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 A	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetLbfo*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetLbfo**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetLbfo**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetNatl**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetNatl**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetQos**, 0, ba3e098, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetSecurity**, 0, ba3e098, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetSwitchTeam**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0lModules\NetSwitchTeam**, 0, ba3e04c, 0, 0, 0) Return: adf7288	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetLbfo\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetLbfo\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetLbfo\t^*, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetNat\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetNat\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetNat\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetNat\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetQos\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShelliv1.0\Modules\NetQos\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShelliv1.0\Modules\NetSecurity\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShelliv1.0\Modules\NetSecurity\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShelliv1.0\Modules\NetSecurity\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShelliv1.0\Modules\NetSwitchTeam\t^*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (\time windir\system32\WindowsPowerShelliv1.0\Modules\NetSwitchTeam\t^*, 0, ba3e04c, 0, 0, 0) Return:	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetLbfo**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetLbfo**, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetNetNot**, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetNat**, 0, ba3e04c, 0, 0, 0) Return: adf7488 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetNat**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetNat**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetQos**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetSecurity**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0Modules\NetTcPIP**, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileE	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetLbfo\v1, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetLbfo\v1, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetLbfo\v1, 0, ba3e098, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetNat\v1, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetNat\v1, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetNat\v1, 0, ba3e088, 0, 0, 0) Return: adf7208 API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetNat\v1, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetSoxtr\v1, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetSecurity\v1, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetSecurity\v1, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetSecurity\v1, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetSecurity\v1, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam\v1, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam\v1, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam\v1, 0, ba3e04c, 0, 0, 0) Return: adf7288 API N	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetLbfo\tangle, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetLbfo\tangle, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetLbfo\tangle, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetNat\tangle, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetNat\tangle, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetNat\tangle, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetQos\tangle, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetGos\tangle, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetGeoxity\tangle, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetGeoxity\tangle, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetGeoxity\tangle, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetGeoxity\tangle, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetGwitchTeam\tangle, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetSwitchTeam\tangle, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetVortConnectivityStatus\tangle, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\sys	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetLbfo\tangle, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetLbfo\tangle, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetNati*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetNati*, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetNati*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetNati*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetNati*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetQosi*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetGosi*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetSecurity*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetSwitchTeam*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetSwitchTeam*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetSwitchTeam*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\NetSwitchTeam*, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetLbfo\tangle, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetLbfo\tangle, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetLbfo\tangle, 0, ba3e04c, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetNat\tangle, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetNat\tangle, 0, 0, 0) Return: adf7408 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetNat\tangle, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetQos\tangle, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetGos\tangle, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetGeoxity\tangle, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetGeoxity\tangle, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetGeoxity\tangle, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetGeoxity\tangle, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetGwitchTeam\tangle, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetSwitchTeam\tangle, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\NetVortConnectivityStatus\tangle, 0, ba3e04c, 0, 0, 0) Return: adf7288 API Name: FindFirstFileExW Args: (%windir%\sys	732 732 732 732 732 732 732 732 732 732	844 844 844 844 844 844 844 844

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\PK(\t^*, 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\t^*, 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\v1, 0, ba3e04c, 0, 0, 0) Return: adf7288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\v1, 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: adf7	732	844
Odii i iiosystom za i	74 Traine: I man had heavy rags. (swindi susystems (white heavy rags) (swindi susystems (swindi susystems) (swindi susyste	702	044
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e04c, 0, 0, 0) Return: adf7 288	732	844
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, ba3e098, 0, 0, 0) Return: adf7	732	844
	408		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 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 T	732	844
	ype: VSDT_COM_DOS		
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 T ype: 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
		2768	2220
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	2/68	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_02c86d53-64d3-405a-b874-3fb9e4d3d801 T ype: 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 T	2768	2220
	ype: VSDT_COM_DOS	2,00	LLLO
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Call System API		732	844
	API Name: GetVersionExA Args: (73a482d0) Return: 1		
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 T ype: 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 T ype: 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 T ype: 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 T		2220
	ype: VSDT_COM_DOS	2768	
Call Network API		732	2704
	ype: VSDT_COM_DOS		
Call Network API	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540	732	2704
Call Network API Write File	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732 2768	2704 2220
Call Network API Write File Write File Write File	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732 2768 2768 2768	2704 2220 2220 2220
Call Network API Write File Write File	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\\discrosoft\\Windows\\PowerShell\\CommandAnalysis\\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\\discrosoft\\Windows\\PowerShell\\CommandAnalysis\\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\\discrosoft\\Windows\\PowerShell\\CommandAnalysis\\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1 Path: %LOCALAPPDATA%\\discrosoft\\Windows\\PowerShell\\CommandAnalysis\\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T	732 2768 2768	2704 2220 2220
Call Network API Write File Write File Write File Call Filesystem API	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1	732 2768 2768 2768 2768	2704 2220 2220 2220 2220
Call Network API Write File Write File Write File Call Filesystem API	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\\discrosoft\\Windows\\PowerShell\\CommandAnalysis\\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\\discrosoft\\Windows\\PowerShell\\CommandAnalysis\\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\\discrosoft\\Windows\\PowerShell\\CommandAnalysis\\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1 Path: %LOCALAPPDATA%\\discrosoft\\Windows\\PowerShell\\CommandAnalysis\\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T	732 2768 2768 2768 2768	2704 2220 2220 2220 2220
Call Network API Write File Write File Write File Call Filesystem API Write File	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T ype: VSDT_COM_DOS	732 2768 2768 2768 2768 2768 732	2704 2220 2220 2220 2220 2220 844
Call Network API Write File Write File Write File Call Filesystem API Write File Write File	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type	732 2768 2768 2768 2768 2768 732	2704 2220 2220 2220 2220 2220 844
Call Network API Write File Write File Write File Call Filesystem API Write File Write File Write File Write File	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type : VSDT_COM_DOS	732 2768 2768 2768 2768 2768 732 732	2704 2220 2220 2220 2220 2220 844 844
Call Network API Write File Write File Write File Call Filesystem API Write File Write File Write File Write File Write File Write File	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type: VSDT_COM_DOS	732 2768 2768 2768 2768 2768 732 732 732 732 2768	2704 2220 2220 2220 2220 2220 844 844 844 844
Call Network API Write File Write File Write File Call Filesystem API Write File Write File Write File Write File Write File	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732 2768 2768 2768 2768 2768 732 732 732	2704 2220 2220 2220 2220 2220 844 844 844
Call Network API Write File Write File Write File Write File Call Filesystem API Write File	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732 2768 2768 2768 2768 2768 732 732 732 732 2768	2704 2220 2220 2220 2220 844 844 844 2220 2220
Call Network API Write File Write File Write File Call Filesystem API Write File	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732 2768 2768 2768 2768 2768 732 732 732 732 2768	2704 2220 2220 2220 2220 2220 844 844 844 844 2220
Call Network API Write File Write File Write File Call Filesystem API Write File	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732 2768 2768 2768 2768 2768 732 732 732 732 2768	2704 2220 2220 2220 2220 844 844 844 2220 2220
Call Network API Write File Write File Write File Write File Call Filesystem API Write File	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\Powe	732 2768 2768 2768 2768 2768 732 732 732 2768 2768 732	2704 2220 2220 2220 2220 844 844 844 2220 2220
Call Network API Write File Write File Write File Write File Call Filesystem API Write File	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1 Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheEntry_7f6a42fc9-f82f-47c6-8c43-f917c96f327f Type : VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type : VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type : VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VS	732 2768 2768 2768 2768 2768 732 732 732 2768 2768 732 2768	2704 2220 2220 2220 2220 844 844 844 2220 2220
Call Network API Write File Write File Write File Write File Call Filesystem API Write File	ype: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: c4 Path: %LOCALAPPDATA%iMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (7d47f78, b92e544) Return: 1 Path: %LOCALAPPDATA%iMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftiWindows\PowerShell\CommandAnalysis\	732 2768 2768 2768 2768 2768 732 732 732 2768 2768 2768 732 732 732 732 732 732	2704 2220 2220 2220 2220 844 844 844 2220 2220

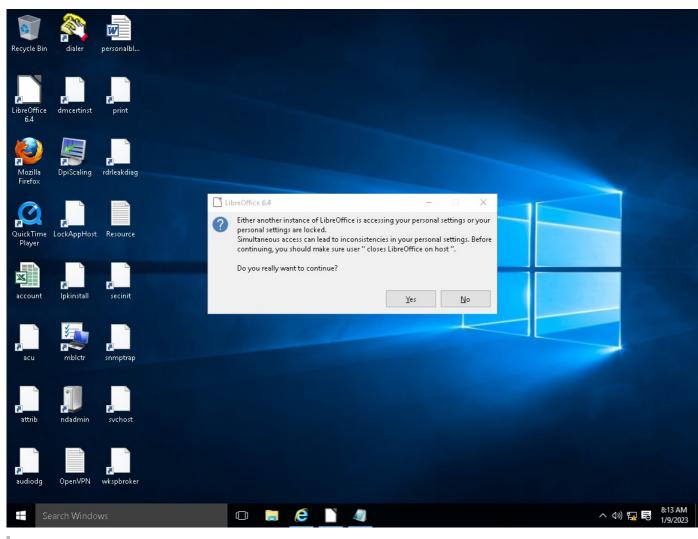
Write File	Path: %LOCALAPPDATA%IMicrosoftlWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%MicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c7b7956f-9ccf-4bdd-9c13-96d73b3795c4 Type: VSDT_COM_DOS	732	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 T ype: 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%iMicrosoftWindows\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 Ty pe: 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 Ty pe: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%MicrosoftWindows\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 T ype: \SDT COM DOS	732	844
Write File	pet. VSD1_COW_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%iMicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bc4b32fd-57c3-413a-a2e1-81be6176e045 T	2768	2220
Write File	ype: VSDT_COM_DOS 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 T ype: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%iMicrosoft\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 T ype: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%iMicrosoftWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_238249d9-828b-47b0-99cf-67b3e0c55472 T ype: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%iMicrosoftlWindows\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 T ype: 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 T ype: 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 T ype: 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 T ype: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%IMicrosoftWindows\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 Write File	API Name: send Args: (c4, A, 69, 0) Return: 69 Path: %LOCALAPPDATA%iMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b95/9b4Fe3e1-4db4-8644-b1ed72179373 T	732 732	2704 844
Write File	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\Power\Shell\CommandAnalysis\Power\Shell_Analysis\CacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%imicrosoftiWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheEntry_bdda54c5-bb1d-49ea-917e-c5e884cf797f T	2768	2220
Write File	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftWindowsiPowerShelliCommandAnalysisiPowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bdda54c5-bb1d-49ea-917e-c5e884cf797fT ype: 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-6dc77b37a861T ype: 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_Analysis\CacheEntry_d4f5287b-0a2b-4513-867d-6dc77b37a861 T ype: 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%iMicrosoft\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 Ty pe: 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 T ype: 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 T ype: 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 T ype: 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 T ype: 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 T ype: 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 T ype: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_051467ba-d833-46ee-91c1-b1d5fee0ebc5 T ype: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_051467ba-d833-46ee-91c1-b1d5fee0ebc5 T ype: 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_Analysis\CacheEntry_9394bfc5-873e-4824-9a5a-5ff7636eb310 Ty pe: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9394bfc5-873e-4824-9a5a-5ff7636eb310 Ty pe: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c64f8295-29ee-4655-8bf9-a42779197977 T ype: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c64f8295-29ee-4655-8bf9-a42779197977 T ype: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7745226a-4a4e-479d-895c-2356425378f7 T ype: 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: (7d47f8, b92e544) Return: 1	2768	2220
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ? API Name: DecOuppi5v Args: (243,103,20,230, 1, 50020000) Patient: 0	732	2704
Call System API	API Name: DnsQueryEx Args: (212,193.30,230, 1, 50020000) Return: 0 API Name: nethosthyrame Arre: (212,193.30,230) Return: 212,193.30, 230	732	2704
Call Network API Call Network API	API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230 API Name: socket Args: (2, 1, 6) Return: c4	732 732	2704
Write File	Path: %LOCALAPPDATA%Microsoft(Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375	2768	2220
WIILE I IIE			
Write File	Type: VSDT_COM_DOS 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 T ype: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%iMicrosofttWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%IMicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c95ec244-f23a-418c-8d6c-f067bf91bc99 Ty	2768	2220
	pe: VSDT_COM_DOS		
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 T ype: VSDT_COM_DOS	2768	2220
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2768	2220
Write File	$Path: \\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	732	844
	ype: VSDT_COM_DOS		
Write File 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%IMicrosoftlWindows\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	732	844
	Type: VSDT_COM_DOS		
Write File	Path: %LOCALAPPDATA%IMicrosoft(Windows)PowerShell/CommandAnalysis/PowerShell_Analysis/CacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%IMicrosoft(Windows)PowerShell/CommandAnalysis/PowerShell_Analysis/CacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%IMicrosoft(Windows)PowerShell/CommandAnalysis/PowerShell_Analysis/CacheIndex 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	044
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	732	844
Write File	Path: %LOCALAPPDATA%IMicrosoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_93bcf22c-e017-4451-8a3c-46a8a03bea81 T	732	844
Write File	ype: VSDT_COM_DOS Path: 9/ LOCALADDDATA9/IM/intercedfil/Mindous/DougleShall/CommontApplysis/DougleShall/Applysis/Coheledgy Ture: VSDT_COM_DOS	799	944
Write File Write File	Path: %LOCALAPPDATA%IMicrosoft(Windows)PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%IMicrosoft(Windows)PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_09fee7e3-7ce5-4af7-8d11-b9304fac801e Ty	732 732	844
write File	pe: VSDT_COM_DOS	732	044
Write File	Path: %LOCALAPPDATA%iMicrosoftiWindows\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 Ty	2768	2220
W = 50	pe: VSDT_COM_DOS	0700	0000
Write File Add File	Path: %LOCALAPPDATA%IMicrosoft(Windows)PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	732	2220 844
Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log Type: VSDT_ASCII	732	844
Call Network API	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log Type: VSDT_ASCII 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: 04	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: ? API Name: DecQuerdev Args: (24, 49, 20, 20, 4, 50020000) Peturo: 0	732	2704
Call System API Call Network API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0 API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732 732	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
	API Name: send Args: (c4, A, 69, 0) Return: 69	732	2704
Call Network API	ADIAI Norman American		2704
Call Network API	API Name: recv Args: (c4, , 4, 0) Return: ?	732	2704
Call Network API Call System API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0	732	2704
Call Network API Call System API Call Network API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0 API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230	732 732	2704
Call Network API Call System API Call Network API Call Network API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0 API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230 API Name: socket Args: (2, 1, 6) Return: c4	732 732 732	2704 2704
Call Network API Call System API Call Network API Call Network API Call Network API Call Network API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0 API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230 API Name: socket Args: (2, 1, 6) Return: c4 API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0	732 732 732 732	2704 2704 2704
Call Network API Call System API Call Network API Call Network API Call Network API Call Network API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0 API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230 API Name: socket Args: (2, 1, 6) Return: c4 API Name: connect Args: (c4, 212.193.30.230.7324, 16) Return: 0 API Name: send Args: (c4, A, 69, 0) Return: 69	732 732 732 732 732	2704 2704 2704 2704
Call Network API Call System API Call Network API	API Name: socket Args: (242.193.30.230, 1, 50020000) Return: 0 API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230 API Name: socket Args: (2, 1, 6) Return: c4 API Name: connect Args: (c4, 212.193.30.230:7324, 16) Return: 0 API Name: send Args: (c4, A, 69, 0) Return: 69 API Name: recv Args: (c4, , 4, 0) Return: ?	732 732 732 732 732 732 732	2704 2704 2704 2704 2704
Call Network API Call System API Call Network API Call Network API Call Network API Call Network API	API Name: DnsQueryEx Args: (212.193.30.230, 1, 50020000) Return: 0 API Name: gethostbyname Args: (212.193.30.230) Return: 212.193.30.230 API Name: socket Args: (2, 1, 6) Return: c4 API Name: connect Args: (c4, 212.193.30.230.7324, 16) Return: 0 API Name: send Args: (c4, A, 69, 0) Return: 69	732 732 732 732 732	2704 2704 2704 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	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B85 5
MD5	D41D8CD98F00B204E9800998ECF8427E
TLSH	-
Size	0 byte(s)

Risk Level Unrated Detection Exploited vulnerabilities

Process Graph Legend

