Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-04-24 14:35:20
Submitter	Manual Submission
Type	WinAce archive

Analysis Overview

Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	TROJ_FRS.0NA103DF21		
Exploited vulnerabilities	-		
Analyzed objects	WinAce archive	1 - Shipping Documents000000000000000000020.ace	C91674FFAED9977654901ABA76E5AC9DE297F6D5
	MSIL Portable executable	1.1 - Shipping Documents000000000000000000020.exe	E67ECFBAE026B6643E2EFB7E22A0B209658D943A

Analysis Environments

	CentOS w Docker	W7	W10
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			

CentOS w Docker

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_FRS.0NA103DF21
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - Shipping Documents000000000000000000020.ace (WinAce archive)

File name	Shipping Documents000000000000000000020.ace
File type	WinAce archive
SHA-1	C91674FFAED9977654901ABA76E5AC9DE297F6D5
SHA-256	549199C8BAF947FF7715FC591C6054F457FC696E6E978403C50203C7A6302BB7
MD5	988103D5C7ACD5511E006FA056D05D60
Size	639703 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

Object 1.1 - Shipping Documents000000000000000000020.exe (MSIL Portable executable)

File name	Shipping Documents000000000000000000020.exe
File type	MSIL Portable executable
SHA-1	E67ECFBAE026B6643E2EFB7E22A0B209658D943A
SHA-256	40295912AEEB49A6C9CB45BF5981E80ED788DE2984E6306CCFD8CBFDC6855C9C
MD5	88926051EB8F9A2FF4AB25CE7A0AD41A
Size	872960 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.0NA103DF21
Exploited vulnerabilities	-
Threat Characteristics	Malformed, defective, or with known malware traits (1)

Notable Threat Characteristics

Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as known malware	■■■	Source: ATSE Detection Name: TROJ_FRS.0NA103DF21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	E67ECFBAE026B6643E2EFB7E22A0B209658D943A	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.0NA103DF21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		

W7

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_FRS.0NA103DF21
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - Shipping Documents00000000000000000020.ace (WinAce archive)

File name	Shipping Documents00000000000000000020.ace
File type	WinAce archive
SHA-1	C91674FFAED9977654901ABA76E5AC9DE297F6D5
SHA-256	549199C8BAF947FF7715FC591C6054F457FC696E6E978403C50203C7A6302BB7
MD5	988103D5C7ACD5511E006FA056D05D60
Size	639703 byte(s)

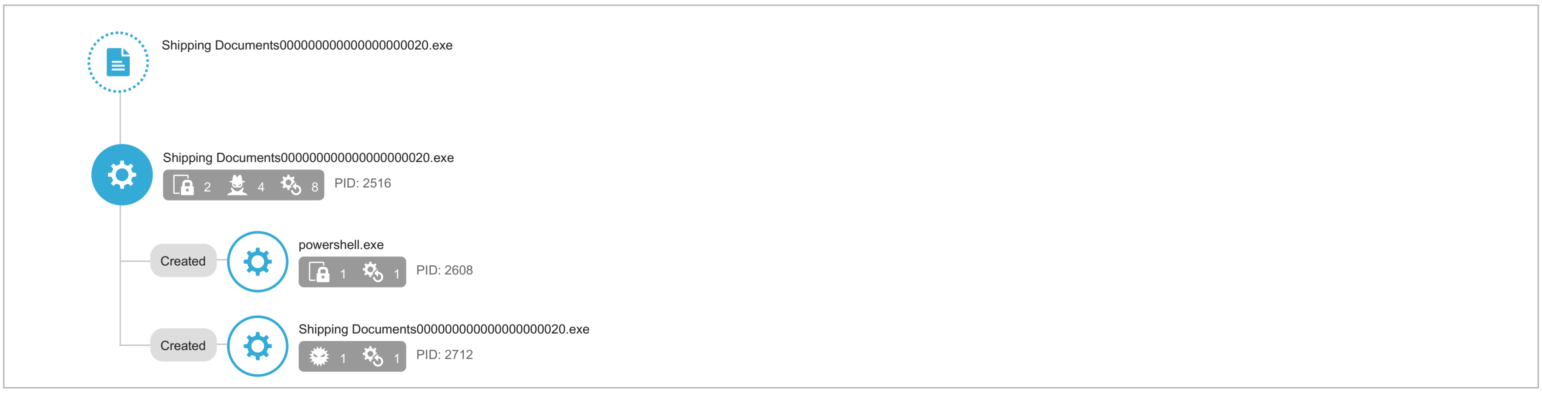
Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

Object 1.1 - Shipping Documents00000000000000000020.exe (MSIL Portable executable)

File name	Shipping Documents00000000000000000020.exe
File type	MSIL Portable executable
SHA-1	E67ECFBAE026B6643E2EFB7E22A0B209658D943A
SHA-256	40295912AEEB49A6C9CB45BF5981E80ED788DE2984E6306CCFD8CBFDC6855C9C
MD5	88926051EB8F9A2FF4AB25CE7A0AD41A
Size	872960 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.0NA103DF21
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (6) Hijack, redirection, or data theft (4) Malformed, defective, or with known malware traits (2) Process, service, or memory object change (10)

Process Graph



Shipping Documents00000000000000000020.exe
Shipping Documents00000000000000000020.exe
2
4
8
PID: 2516
Created
powershell.exe
1
1
PID: 2608
Created
Shipping Documents00000000000000000020.exe
1
1
PID: 2712

Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics	
Execution	Windows Management Instrumentation	🟥⬜⬜ Characteristics:	1, 2, 3, 4
	PowerShell	🟥⬜⬜ Characteristics:	1
	Execution through API	🟥⬜⬜ Characteristics:	1
Privilege Escalation	Process Injection	🟥🟥⬜ Characteristics: 🟥⬜⬜ Characteristics:	1, 2 1, 2
Defense Evasion	Software Packing	🟥⬜⬜ Characteristics:	1
	Process Injection	🟥🟥⬜ Characteristics: 🟥⬜⬜ Characteristics:	1, 2 1, 2
	Process Hollowing	🟥⬜⬜ Characteristics:	1
Discovery	Process Discovery	🟥⬜⬜ Characteristics:	1, 2
	System Information Discovery	🟥⬜⬜ Characteristics:	1, 2, 3, 4

Notable Threat Characteristics

Anti-security, self-preservation (6)

Characteristic	Significance	Details
Attempts to detect active running processes	🟥⬜⬜	Process ID: 2608 Info: enum processes
Attempts to detect active running processes	🟥⬜⬜	Process ID: 2516 Info: enum processes
Attempts to detect sandbox application modules	🟥⬜⬜	Process ID: 2516 Module: SbieDll.dll
Attempts to detect sandbox characteristics	🟥⬜⬜	Sample attempted to detect sandbox using the following registry item: [SOFTWARE\VMware, Inc.\VMware Tools\]
Attempts to detect sandbox characteristics	🟥⬜⬜	Sample attempted to detect sandbox using the following registry item: [SOFTWARE\Oracle\VirtualBox Guest Additions\]
Uses suspicious packer	🟥⬜⬜	File Name: %WorkingDir%\Shipping Documents000000000000000000020.exe Packer: UNKNOWN

▼ Hijack, redirection, or data theft (4)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2516 Info: Obtains Description from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2516 Info: Obtains __PATH from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2516 Info: Obtains __GENUS from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2516 Info: Obtains Win32_VideoController from API result

▼ Malformed, defective, or with known malware traits (2)

Characteristic	Significance	Details
Causes process to crash	🟥⬜⬜	Process ID: 2712 Image Path: Shipping Documents000000000000000000020.exe
Detected as known malware	🟥🟥🟥	Source: ATSE Detection Name: TROJ_FRS.0NA103DF21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

▼ Process, service, or memory object change (10)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 2712 Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe
Creates process	🟥⬜⬜	Process ID: 2516 Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Shell Command:
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2516 Injected API: WriteProcessMemory Target Process ID: 2712 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2516 Injected API: SetThreadContext Target Process ID: 2712 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2516 Target Process ID: 2712 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Address: 0x0
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2516 Target Process ID: 2712 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Content:
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2516 Target Process ID: 2712 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Content: .u.
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 2516 Target Process ID: 2712 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Content: MZ.
Injects memory with dropped files	🟥⬜⬜	Injecting Process ID: 2516 Target Process ID: 2712 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe File: MZ.
Creates process in system directory	🟥⬜⬜	Process ID: 2608 Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %WorkingDir%\Shipping Documents000000000000000000020.exe

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
iecvlist.microsoft.com	152.199.19.161	53	-	No risk	-	Shipping Documents000000000000000000020.exe
ie9cvlist.ie.microsoft.com	152.199.19.161	53	-	No risk	-	Shipping Documents000000000000000000020.exe
iecvlist.microsoft.com	152.199.19.161	443	-	-	-	Shipping Documents000000000000000000020.exe
iecvlist.microsoft.com	152.199.19.161	80	-	-	-	Shipping Documents000000000000000000020.exe

URL	Site Category	Risk Level	Threat	Accessed By
http://ie9cvlist.ie.microsoft.com/IE9CompatViewList.xml	Business / Economy Computers / Internet Cloud Applications	No risk	-	Shipping Documents000000000000000000020.exe

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
3Z5TF50V1PX7L036PLZE.temp	No risk	-	-	-	8016	B6C3D6DA92C65D02FAE4E8166C04A22322946475
d93f411851d7c929.customDestinations-ms	No risk	-	-	-	8016	B6C3D6DA92C65D02FAE4E8166C04A22322946475
d93f411851d7c929.customDestinations-ms~RF1d0ad7.TMP	No risk	-	-	-	8016	E8FEC2936251809B10A7D035E842FA074562114B

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	E67ECFBAE026B6643E2EFB7E22A0B209658D943A	High

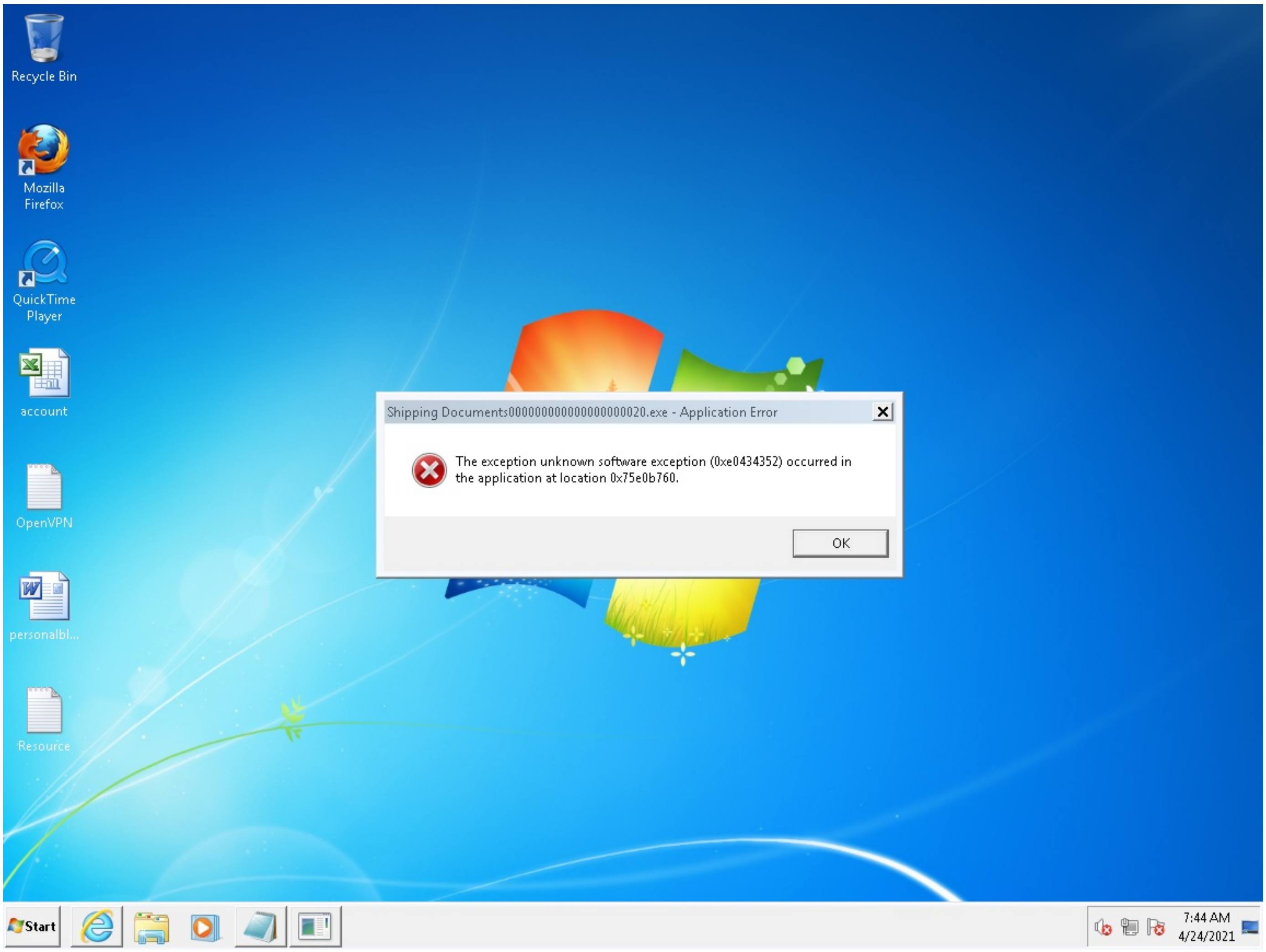
Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.0NA103DF21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\Shipping Documents000000000000000000020.exe Packer: UNKNOWN		
Call System API	API Name: CryptExportKey Args: (305fd0, 0, 6, 0, 0, 18cda8) Return: 1		2516
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2516
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2516
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2516
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 93782392, 8) Return: 0		2516
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 93782432, 8) Return: 0		2516
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 93782472, 8) Return: 0		2516
Call System API	API Name: EnumProcesses Args: () Return: 1		2516
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2516 Info: enum processes		
Call Thread API	API Name: NtResumeThread Args: (Process:2608,) Return: ?		2516
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2608], ppid[2516) Return: 1		2516
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.exe, "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%WorkingDir%\Shipping Documents000000000000000000020.exe", , , , , , %WorkingDir%, SW_HIDE, Process:2608:%windir%\System32\WindowsPowerShell\v1.0\powershell.exe) Return: 1		2516
Read Registry Key	Key: SOFTWARE\Oracle\VirtualBox Guest Additions\ Value: None		2516
Detection	Threat Characteristic: Attempts to detect sandbox characteristics Sample attempted to detect sandbox using the following registry item: [SOFTWARE\Oracle\VirtualBox Guest Additions\]		
Read Registry Key	Key: SOFTWARE\VMware, Inc.\VMware Tools\ Value: None		2516
Detection	Threat Characteristic: Attempts to detect sandbox characteristics Sample attempted to detect sandbox using the following registry item: [SOFTWARE\VMware, Inc.\VMware Tools\]		
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\ROOT\cimv2, en-US,en, 0, 0, 7d0e8dc) Return: 0		2516
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\ROOT\cimv2, NULL, NULL, , 80, , 0, 7d0e8dc) Return: 0		2516
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_VideoController, 10, 0, 18b578) Return: 0		2516
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2516 Info: Obtains Win32_VideoController from API result		
Detection	Threat Characteristic: Creates process in system directory Process ID: 2608 Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %WorkingDir%\Shipping Documents000000000000000000020.exe		
Call WMI API	API Name: Win32_VideoController::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0		2516
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2516 Info: Obtains __GENUS from API result		
Call WMI API	API Name: Win32_VideoController::Get Args: (__PATH, 0, \\Win-Magnus\ROOT\cimv2:Win32_VideoController.DeviceID="VideoController1", 8, 64) Return: 0		2516
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2516 Info: Obtains __PATH from API result		
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Standard VGA Graphics Adapter, 8, 0) Return: 0		2516
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2516 Info: Obtains Description from API result		
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Standard VGA Graphics Adapter, 8, 0) Return: 0		2516
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Standard VGA Graphics Adapter, 8, 0) Return: 0		2516
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\46\52C64B7E\LanguageList Value: en-US\0en\0	2516	2608
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 727b0250, -1, 15eb60, 15eb5c, 0) Return: 0	2516	2608

Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms) Return: 1	2516	2608
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1d0ad7.TMP) Return: 1	2516	2608
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\3Z5TF50V1PX7L036PLZE.temp Type: VSDT_COM_DOS	2516	2608
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\3Z5TF50V1PX7L036PLZE.temp Type: VSDT_COM_DOS	2516	2608
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1d0ad7.TMP Type: VSDT_EMPTY	2516	2608
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1d0ad7.TMP Type: VSDT_COM_DOS	2516	2608
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms Type: VSDT_COM_DOS	2516	2608
Delete File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1d0ad7.TMP Type: VSDT_COM_DOS	2516	2608
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Standard VGA Graphics Adapter, 8, 0) Return: 0		2516
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Standard VGA Graphics Adapter, 8, 0) Return: 0		2516
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Standard VGA Graphics Adapter, 8, 0) Return: 0		2516
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Standard VGA Graphics Adapter, 8, 0) Return: 0		2516
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Standard VGA Graphics Adapter, 8, 0) Return: 0		2516
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Standard VGA Graphics Adapter, 8, 0) Return: 0		2516
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Standard VGA Graphics Adapter, 8, 0) Return: 0		2516
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Standard VGA Graphics Adapter, 8, 0) Return: 0		2516
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Standard VGA Graphics Adapter, 8, 0) Return: 0		2516
Call System API	API Name: GetModuleHandleA Args: (SbieDll.dll) Return: 0		2516
Detection	Threat Characteristic: Attempts to detect sandbox application modules Process ID: 2516 Module: SbieDll.dll		
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\Shipping Documents000000000000000000020.exe, , , , , CREATE_SUSPENDED, , , , Process:2712:%WorkingDir%\Shipping Documents000000000000000000020.exe) Return: 1		2516
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2516 Injected API: WriteProcessMemory Target Process ID: 2712 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe		
Detection	Threat Characteristic: Creates process Process ID: 2516 Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2712:%WorkingDir%\Shipping Documents000000000000000000020.exe, 400000, MZ., 512, 18b9a8) Return: 1		2516
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2516 Target Process ID: 2712 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2516 Target Process ID: 2712 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2712:%WorkingDir%\Shipping Documents000000000000000000020.exe, 402000, .u., 219136, 18b9a8) Return: 1		2516
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2516 Target Process ID: 2712 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Content: .u.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2712:%WorkingDir%\Shipping Documents000000000000000000020.exe, 438000, , 1024, 18b9a8) Return: 1		2516
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2516 Target Process ID: 2712 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Content:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2712:%WorkingDir%\Shipping Documents000000000000000000020.exe, 43a000, , 512, 18b9a8) Return: 1		2516
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7ffdf000 Process:2712:%WorkingDir%\Shipping Documents000000000000000000020.exe, 7ffdf008, , 4, 18b9a8) Return: 1		2516
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2516 Target Process ID: 2712 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2712:%WorkingDir%\Shipping Documents000000000000000000020.exe) Return: 1		2516
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2516 Injected API: SetThreadContext Target Process ID: 2712 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:2712,) Return: ?		2516
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2712], ppid[2516) Return: 1		2516
Call Systeminfo API	API Name: NtQuerySystemInformation Args: (5, , 131072, 45264) Return: 0	2516	2608
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2608 Info: enum processes		
Call System API	API Name: CryptExportKey Args: (326250, 0, 6, 0, 0, 15ebc0) Return: 1	2516	2608
Detection	Threat Characteristic: Creates process Process ID: 2712 Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe		
Call Filesystem API	API Name: DeleteFileW Args: (%windir%\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.2608.1903475) Return: 0	2516	2608

Call Filesystem API	API Name: DeleteFileW Args: (%windir%\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.2608.1903475) Return: 0	2516	2608
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2608.1903475) Return: 0	2516	2608
Detection	Threat Characteristic: Causes process to crash Process ID: 2712 Image Path: Shipping Documents000000000000000000020.exe		

▼ Screenshot



Shipping Documents000000000000000000020.exe - Application Error

The exception unknown software exception (0xe0434352) occurred in the application at location 0x75e0b760.

W10

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_FRS.0NA103DF21
Exploited vulnerabilities	-
Network connection	Custom

▼ Object 1 - Shipping Documents000000000000000000020.ace (WinAce archive)

File name	Shipping Documents000000000000000000020.ace
File type	WinAce archive
SHA-1	C91674FFAED9977654901ABA76E5AC9DE297F6D5
SHA-256	549199C8BAF947FF7715FC591C6054F457FC696E6E978403C50203C7A6302BB7
MD5	988103D5C7ACD5511E006FA056D05D60
Size	639703 byte(s)

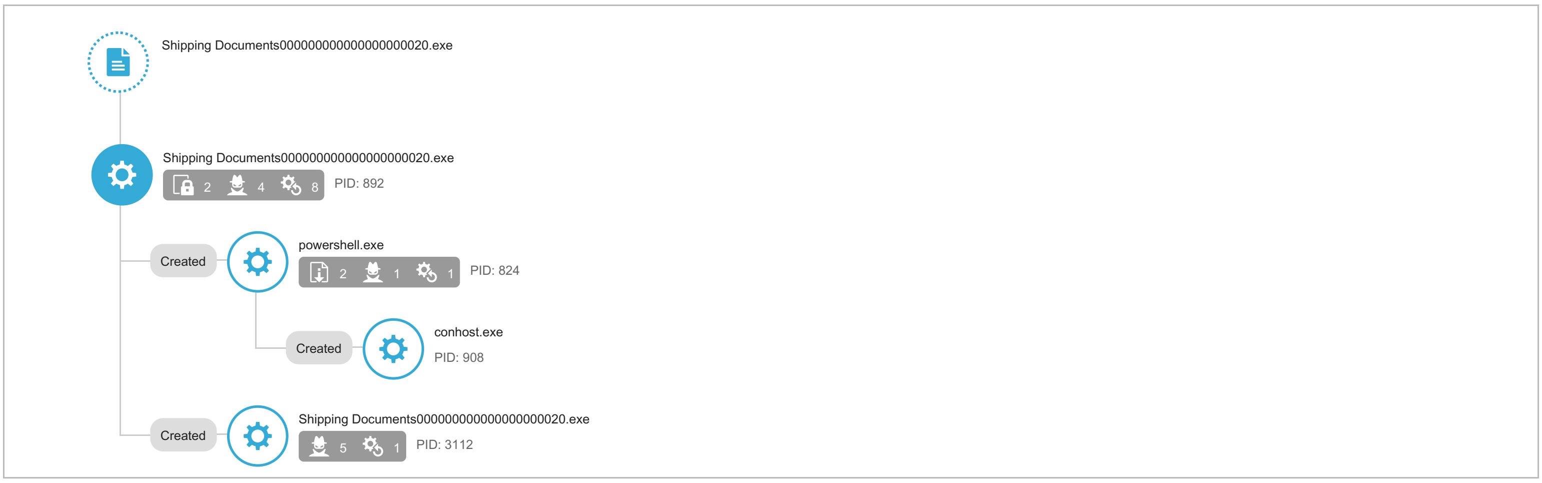
Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

▼ Object 1.1 - Shipping Documents000000000000000000020.exe (MSIL Portable executable)

File name	Shipping Documents000000000000000000020.exe
File type	MSIL Portable executable
SHA-1	E67ECFBAE026B6643E2EFB7E22A0B209658D943A
SHA-256	40295912AEEB49A6C9CB45BF5981E80ED788DE2984E6306CCFD8CBFDC6855C9C
MD5	88926051EB8F9A2FF4AB25CE7A0AD41A
Size	872960 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.0NA103DF21
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (5) Autostart or other system reconfiguration (2) File drop, download, sharing, or replication (2) Hijack, redirection, or data theft (17) Malformed, defective, or with known malware traits (1) Process, service, or memory object change (11)

Process Graph


Shipping Documents000000000000000000020.exe
Shipping Documents000000000000000000020.exe
2
4
8
PID: 892
Created
powershell.exe
2
1
1
PID: 824
Created
conhost.exe
PID: 908
Created
Shipping Documents000000000000000000020.exe
5
1
PID: 3112

Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics	
Execution	Windows Management Instrumentation	🟥⬜⬜ Characteristics:	1, 2, 3, 4, 5, 6, 7, 8, 9
	PowerShell	🟥⬜⬜ Characteristics:	1
	Execution through API	🟥⬜⬜ Characteristics:	1
Privilege Escalation	Process Injection	🟥🟥⬜ Characteristics: 🟥⬜⬜ Characteristics:	1, 2 1, 2
Defense Evasion	Software Packing	🟥⬜⬜ Characteristics:	1
	Process Injection	🟥🟥⬜ Characteristics: 🟥⬜⬜ Characteristics:	1, 2 1, 2
	Process Hollowing	🟥⬜⬜ Characteristics:	1
	File Deletion	🟥⬜⬜ Characteristics:	1, 2
Discovery	Process Discovery	🟥⬜⬜ Characteristics:	1
	System Information Discovery	🟥⬜⬜ Characteristics:	1, 2, 3, 4, 5, 6, 7, 8, 9
Collection	Data from Local System	🟥⬜⬜ Characteristics:	1, 2, 3, 4, 5, 6

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (5)

Characteristic	Significance	Details
Attempts to detect sandbox application modules	🟥⬜⬜	Process ID: 892 Module: SbieDll.dll
Attempts to detect sandbox characteristics	🟥⬜⬜	Sample attempted to detect sandbox using the following registry item: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware Tools\]
Attempts to detect sandbox characteristics	🟥⬜⬜	Sample attempted to detect sandbox using the following registry item: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oracle\VirtualBox Guest Additions\]
Attempts to detect active running processes	🟥⬜⬜	Process ID: 892 Info: enum processes
Uses suspicious packer	🟥⬜⬜	File Name: %WorkingDir%\Shipping Documents000000000000000000020.exe Packer: UNKNOWN

▼ Autostart or other system reconfiguration (2)

Characteristic	Significance	Details
Modifies important registry entries to perform rogue functions	🟥🟥⬜	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥🟥⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE

▼ File drop, download, sharing, or replication (2)

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 824 File: %TEMP%\nmkyba35.dx3.psm1 Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 824 File: %TEMP%\stgrifwy.cog.ps1 Type: VSDT_ASCII

▼ Hijack, redirection, or data theft (17)

Characteristic	Significance	Details
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\key3.db
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\profiles.ini
Accesses decoy file	🟥⬜⬜	%APPDATA%\FILEZILLA\RECENTSERVERS.XML
Accesses decoy file	🟥⬜⬜	%APPDATA%\COMODO\ICEDRAGON\PROFILES.INI
Accesses decoy file	🟥⬜⬜	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data
Modifies configuration files to perform rogue functions	🟥🟥⬜	%windir%\System32\drivers\etc\hosts
Modifies configuration files to perform rogue functions	🟥🟥⬜	File: %windir%\SYSTEM32\DRIVERS\ETC\HOSTS Modified Content: 127.0.0.1
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3112 Info: Obtains processorID from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3112 Info: Obtains __PATH from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3112 Info: Obtains __GENUS from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3112 Info: Obtains __CLASS from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3112 Info: Obtains SerialNumber from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 892 Info: Obtains Description from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 892 Info: Obtains __PATH from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 892 Info: Obtains __GENUS from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 892 Info: Obtains Win32_VideoController from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 824 Info: Searches files by API

Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as known malware	🟥🟥🟥	Source: ATSE Detection Name: TROJ_FRS.0NA103DF21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

Process, service, or memory object change (11)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 3112 Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe
Creates process	🟥⬜⬜	Process ID: 892 Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Shell Command:
Creates named pipe	🟥⬜⬜	\\.\pipe\PSHost.132637489322430983.824.DefaultAppDomain.powershell
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 892 Injected API: WriteProcessMemory Target Process ID: 3112 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 892 Injected API: SetThreadContext Target Process ID: 3112 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 892 Target Process ID: 3112 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Address: 0x0
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 892 Target Process ID: 3112 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Content:
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 892 Target Process ID: 3112 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Content: .u.
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 892 Target Process ID: 3112 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Content: MZ.
Injects memory with dropped files	🟥⬜⬜	Injecting Process ID: 892 Target Process ID: 3112 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe File: MZ.
Creates process in system directory	🟥⬜⬜	Process ID: 824 Image Path: %windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%WorkingDir%\Shipping Documents000000000000000000020.exe"

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ocsp.digicert.com	93.184.220.29	53	-	No risk	-	Shipping Documents00000000000000000020.exe
iecvlist.microsoft.com	152.199.19.161	53	-	No risk	-	Shipping Documents00000000000000000020.exe
go.microsoft.com	2.19.113.71	53	-	No risk	-	Shipping Documents00000000000000000020.exe
ctldl.windowsupdate.com	67.26.5.254	53	-	No risk	-	Shipping Documents00000000000000000020.exe
sqm.telemetry.microsoft.com	65.55.252.93	53	-	No risk	-	Shipping Documents00000000000000000020.exe
ieonline.microsoft.com	204.79.197.200	53	-	No risk	-	Shipping Documents00000000000000000020.exe
ocsp.digicert.com	93.184.220.29	80	-	-	-	Shipping Documents00000000000000000020.exe
go.microsoft.com	2.19.113.71	80	-	-	-	Shipping Documents00000000000000000020.exe
ctldl.windowsupdate.com	8.253.193.121	80	-	-	-	Shipping Documents00000000000000000020.exe
ctldl.windowsupdate.com	8.253.193.241	80	-	-	-	Shipping Documents00000000000000000020.exe
sqm.telemetry.microsoft.com	65.55.252.93	443	-	-	-	Shipping Documents00000000000000000020.exe
ieonline.microsoft.com	204.79.197.200	443	-	-	-	Shipping Documents00000000000000000020.exe
iecvlist.microsoft.com	152.199.19.161	443	-	-	-	Shipping Documents00000000000000000020.exe

URL	Site Category	Risk Level	Threat	Accessed By
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?814b3008d3fcbcb4	Computers / Internet Cloud Applications	No risk	-	Shipping Documents00000000000000000020.exe
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?c2fdfc76156fab7f	Computers / Internet Cloud Applications	No risk	-	Shipping Documents00000000000000000020.exe
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9ef9ee26956a1a8a	Computers / Internet Cloud Applications	No risk	-	Shipping Documents00000000000000000020.exe
http://go.microsoft.com/fwlink/?LinkID=401135	Computers / Internet	No risk	-	Shipping Documents00000000000000000020.exe
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8UIl8gIGmZT9XHrHiJQeI%3D	Computers / Internet Cloud Applications	No risk	-	Shipping Documents00000000000000000020.exe

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
stgrifwy.cog.ps1	No risk	-	-	-	1	356A192B7913B04C54574D18C28D46E6395428AB
d93f411851d7c929.customDestinations-ms	No risk	-	-	-	6213	A366778B5C05B368D4CD50D22E2AAED8F9BB47F8
d93f411851d7c929.customDestinations-ms~RF1a89f.TMP	No risk	-	-	-	6213	FBC4D6995121320C454BEE7C1D6998AAD190B483
62RH06GL4F7ZRROLSH1Y.temp	No risk	-	-	-	6213	A366778B5C05B368D4CD50D22E2AAED8F9BB47F8
PowerShell_AnalysisCacheEntry_f95ace63-33bc-4cea-a2a4-826cd72e8851	No risk	-	-	-	4494	0B392D926A964596C26121F4CB3293BD36EE9141
PowerShell_AnalysisCacheEntry_18c9fb0c-fb68-4c86-bcd4-a92ef5adf42b	No risk	-	-	-	2230	B5E2A57FF7BF9B686B49EB471B2849252B5062BA
PowerShell_AnalysisCacheEntry_57a19812-ad31-47d3-b27b-900612eb602c	No risk	-	-	-	336	B3F0AFCF9B1A3519FC1E9E972982E258C2FEEC05
PowerShell_AnalysisCacheEntry_623a97e5-a4a4-466d-9768-cbb2f5fe0748	No risk	-	-	-	6458	4690A032A1CC6C3CF0514873D58E67B652108F9A
PowerShell_AnalysisCacheIndex	No risk	-	-	-	21073	6B0C1B13D48639DCA5B96D180A75222F8BAEC095
PowerShell_AnalysisCacheEntry_505d4d03-80d5-49a8-bbf5-d1da70a946da	No risk	-	-	-	18095	E46427FE2A443582845B184BD204F4E6096CE788

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	E67ECFBAE026B6643E2EFB7E22A0B209658D943A	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.0NA103DF21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\Shipping Documents00000000000000000020.exe Packer: UNKNOWN		
Call System API	API Name: System.Convert::FromBase64String Args: (AAEAAAD/////AQAAAAAAAAAEAQAAAI4BU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuTGlzdGAxW1tTeXN0ZW0uU2VjdXJpdHkuQ2xhaW1zLkNsYWltLCBtc2Nvcmxp...) Return: 0001000000FFFFFF...		892
Call System API	API Name: System.Convert::FromBase64String Args: (AAEAAAD/////AQAAAAAAAAAEAQAAAH9TeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5MaXN0YDFbW1N5c3RlbS5TdHJpbmcsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4w...) Return: 0001000000FFFFFF...		892

Call System API	API Name: System.Convert::FromBase64String Args: (AAEAAAD/////AQAAAAAAAAAEAQAAACVTeXN0ZW0uU2VjdXJpdHkuQ2xhaW1zLkNsYWltc0lkZW50aXR5CAAAAAltX3ZlcnNpb24HbV9hY3RvchRtX2F1dGhlbnRpY2F0...) Return: 0001000000FFFFFF...		892
Call System API	API Name: System.Convert::FromBase64String Args: (AAEAAAD/////AQAAAAAAAAAEAQAAAI4BU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuTGlzdGAxW1tTeXN0ZW0uU2VjdXJpdHkuQ2xhaW1zLkNsYWltLCBtc2Nvcmxp...) Return: 0001000000FFFFFF...		892
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		892
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		892
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		892
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 186777976, 8) Return: 0		892
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 186778016, 8) Return: 0		892
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 186778056, 8) Return: 0		892
Call System API	API Name: EnumProcesses Args: () Return: 1		892
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 892 Info: enum processes		
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		892
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		892
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.exe, "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%WorkingDir%\Shipping Documents000000000000000000020.exe", , , , CREATE_SUSPENDED, , %WorkingDir%, SW_HIDE, Process:824:%windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe) Return: 1		892
Call Thread API	API Name: NtResumeThread Args: (Process:824,) Return: ?		892
Call System API	API Name: evtchann.SendEvent Args: (e), pid[824], ppid[892) Return: 1		892
Read Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oracle\VirtualBox Guest Additions\ Value: None		892
Detection	Threat Characteristic: Attempts to detect sandbox characteristics Sample attempted to detect sandbox using the following registry item: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oracle\VirtualBox Guest Additions\]		
Read Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware Tools\ Value: None		892
Detection	Threat Characteristic: Attempts to detect sandbox characteristics Sample attempted to detect sandbox using the following registry item: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware Tools\]		
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\ROOT\cimv2, en-US,en, 0, b093b18, 1240f078) Return: 0		892
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\ROOT\cimv2, NULL, NULL, , 80, , 0, 1240f078) Return: 0		892
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_VideoController, 10, 0, 46c508) Return: 0		892
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 892 Info: Obtains Win32_VideoController from API result		
Call WMI API	API Name: Win32_VideoController::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0		892
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 892 Info: Obtains __GENUS from API result		
Call WMI API	API Name: Win32_VideoController::Get Args: (__PATH, 0, \\FIN-Adam-Serve\ROOT\cimv2:Win32_VideoController.DeviceID="VideoController1", 8, 64) Return: 0		892
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 892 Info: Obtains __PATH from API result		
Detection	Threat Characteristic: Creates process in system directory Process ID: 824 Image Path: %windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%WorkingDir%\Shipping Documents000000000000000000020.exe"		
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Microsoft Basic Display Adapter, 8, 0) Return: 0		892
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 892 Info: Obtains Description from API result		
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Microsoft Basic Display Adapter, 8, 0) Return: 0		892
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	892	824
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	892	824
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6a499b90, -1, e8e14c, e8e148, 0) Return: 0	892	824
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms) Return: 1	892	824
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1a89f.TMP) Return: 1	892	824
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\62RH06GL4F7ZRROLSH1Y.temp Type: VSDT_COM_DOS	892	824
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\62RH06GL4F7ZRROLSH1Y.temp Type: VSDT_COM_DOS	892	824
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1a89f.TMP Type: VSDT_EMPTY	892	824
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1a89f.TMP Type: VSDT_COM_DOS	892	824
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms Type: VSDT_COM_DOS	892	824
Delete File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1a89f.TMP Type: VSDT_COM_DOS	892	824
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Microsoft Basic Display Adapter, 8, 0) Return: 0		892
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Microsoft Basic Display Adapter, 8, 0) Return: 0		892
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Microsoft Basic Display Adapter, 8, 0) Return: 0		892
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Microsoft Basic Display Adapter, 8, 0) Return: 0		892
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Microsoft Basic Display Adapter, 8, 0) Return: 0		892
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Microsoft Basic Display Adapter, 8, 0) Return: 0		892
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Microsoft Basic Display Adapter, 8, 0) Return: 0		892
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Microsoft Basic Display Adapter, 8, 0) Return: 0		892
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Microsoft Basic Display Adapter, 8, 0) Return: 0		892
Call WMI API	API Name: Win32_VideoController::Get Args: (Description, 0, Microsoft Basic Display Adapter, 8, 0) Return: 0		892
Call System API	API Name: GetModuleHandleA Args: (SbieDll.dll) Return: 0		892
Detection	Threat Characteristic: Attempts to detect sandbox application modules Process ID: 892 Module: SbieDll.dll		

Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\Shipping Documents000000000000000000020.exe, , , , , CREATE_SUSPENDED, , , , Process:3112:%WorkingDir%\Shipping Documents000000000000000000020.exe) Return: 1		892
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 892 Injected API: WriteProcessMemory Target Process ID: 3112 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe		
Detection	Threat Characteristic: Creates process Process ID: 892 Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3112:%WorkingDir%\Shipping Documents000000000000000000020.exe, 400000, MZ., 512, 46c934) Return: 1		892
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 892 Target Process ID: 3112 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 892 Target Process ID: 3112 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3112:%WorkingDir%\Shipping Documents000000000000000000020.exe, 402000, .u., 219136, 46c934) Return: 1		892
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 892 Target Process ID: 3112 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Content: .u.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3112:%WorkingDir%\Shipping Documents000000000000000000020.exe, 438000, , 1024, 46c934) Return: 1		892
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 892 Target Process ID: 3112 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Content:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3112:%WorkingDir%\Shipping Documents000000000000000000020.exe, 43a000, , 512, 46c934) Return: 1		892
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7f80f000 Process:3112:%WorkingDir%\Shipping Documents000000000000000000020.exe, 7f80f008, , 4 , 46c934) Return: 1		892
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 892 Target Process ID: 3112 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:3112:%WorkingDir%\Shipping Documents000000000000000000020.exe) Return: 1		892
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 892 Injected API: SetThreadContext Target Process ID: 3112 Target Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:3112,) Return: ?		892
Call System API	API Name: evtchann.SendEvent Args: (e), pid[3112], ppid[892) Return: 1		892
Call Filesystem API	API Name: CreateNamedPipeW Args: (\\.\pipe\PSHost.132637489322430983.824.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 15259096) Return: 51c	892	824
Detection	Threat Characteristic: Creates named pipe \\.\pipe\PSHost.132637489322430983.824.DefaultAppDomain.powershell		
Detection	Threat Characteristic: Creates process Process ID: 3112 Image Path: %WorkingDir%\Shipping Documents000000000000000000020.exe		
Add File	Path: %TEMP%\stgrifwy.cog.ps1 Type: VSDT_ASCII	892	824
Write File	Path: %TEMP%\stgrifwy.cog.ps1 Type: VSDT_ASCII	892	824
Add File	Path: %TEMP%\nmkyba35.dx3.psm1 Type: VSDT_ASCII	892	824
Write File	Path: %TEMP%\nmkyba35.dx3.psm1 Type: VSDT_ASCII	892	824
Add File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\Shipping Documents000000000000000000020.exe.log Type: VSDT_ASCII		892
Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\Shipping Documents000000000000000000020.exe.log Type: VSDT_ASCII		892
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\stgrifwy.cog.ps1) Return: 1	892	824
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\nmkyba35.dx3.psm1) Return: 1	892	824
Call Service API	API Name: OpenServiceW Args: (7de2490, CryptSvc, 5) Return: 7de2580	892	824
Delete File	Path: %TEMP%\stgrifwy.cog.ps1 Type: VSDT_ASCII	892	824
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 824 File: %TEMP%\stgrifwy.cog.ps1 Type: VSDT_ASCII		
Delete File	Path: %TEMP%\nmkyba35.dx3.psm1 Type: VSDT_ASCII	892	824
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 824 File: %TEMP%\nmkyba35.dx3.psm1 Type: VSDT_ASCII		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\7d\52C64B7E\LanguageList Value: en-US\0en\0	892	824
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	892	824
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	892	824
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	892	824

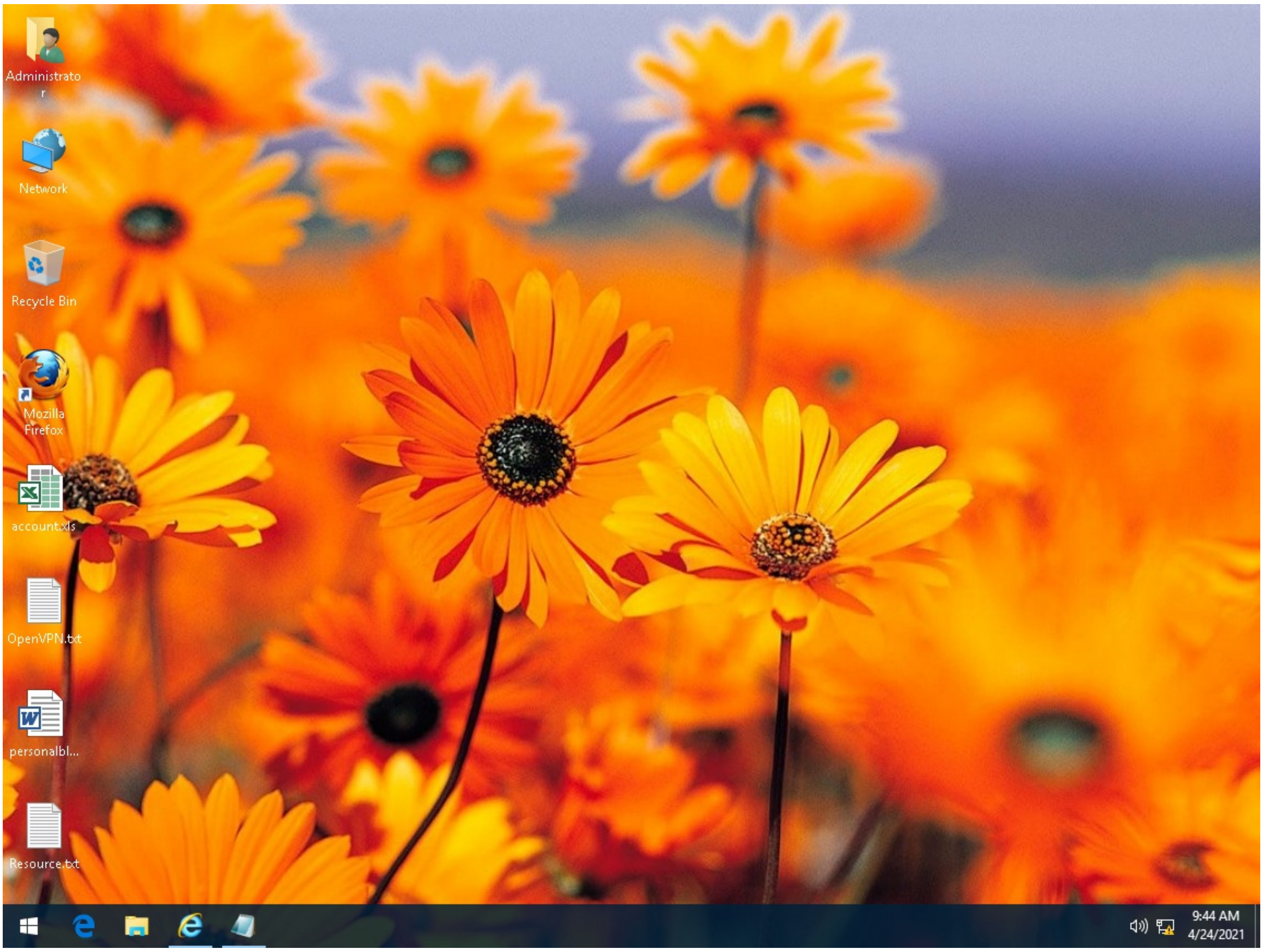
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_367d7386-cb1c-48bb-b1a1-a342e4e50d4c Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_505d4d03-80d5-49a8-bbf5-d1da70a946da Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f2c42dea-0f9a-4e74-873c-b73e8713d7d8 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e116839a-2b1b-4588-be88-517689cfa536 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4d245eee-143c-43e2-ab9a-eca01a38cb58 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\*, 0, b21e094, 0, 0, 0) Return: 7e12f18	892	824
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 824 Info: Searches files by API		
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c3cf3f6b-0abc-48ab-b19c-87f39e281542 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_59996910-2bae-4b01-8439-8432fd48cc45 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_37b04d57-604b-4960-afa4-a38a1594c1a7 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Call Filesystem API	API Name: GetFileAttributesW Args: (%windir%\system32\WinMetadata\Windows.System.UserProfile.winmd) Return: -1	892	824
Call Filesystem API	API Name: GetFileAttributesW Args: (%windir%\system32\WinMetadata\Windows.System.winmd) Return: 32	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d63980c8-601d-4081-80ab-dd5918e3af7a Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_60229287-003e-415b-8b53-4961c9d4dc01 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1f76fb9f-ad8c-4ca8-a94e-898625bb2e86 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_72c9d763-81a0-4efc-bc24-efae2d358d92 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 13cb798, 104eb1c) Return: 0	892	3112
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, NULL, 0, NULL, 0, 104eb1c) Return: 0	892	3112
Call WMI API	API Name: Win32_BaseBoard::Get Args: (SerialNumber, 0, O0IYNPXNRRJEDF, 8, 0) Return: 0	892	3112
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3112 Info: Obtains SerialNumber from API result		
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 13cb098, 6bef6f8) Return: 0	892	3112
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, , 80, , 0, 6bef6f8) Return: 0	892	3112
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ea6be6b9-079e-4a17-998a-b7bbcb6acfb1 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Call WMI API	API Name: Win32_Processor::Get Args: (__PATH, 0, \\FIN-Adam-Serve\ROOT\cimv2:Win32_Processor, 8, 64) Return: 0	892	3112
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3112 Info: Obtains __PATH from API result		
Call WMI API	API Name: Win32_Processor::Get Args: (__CLASS, 0, Win32_Processor, 8, 64) Return: 0	892	3112
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3112 Info: Obtains __CLASS from API result		
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f95ace63-33bc-4cea-a2a4-826cd72e8851 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_18c9fb0c-fb68-4c86-bcd4-a92ef5adf42b Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f904c07d-6234-4aaf-be8c-60559340f496 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_86a435ed-b36b-4c64-874a-968e2ab7ee47 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Call WMI API	API Name: Win32_Processor::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	892	3112
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3112 Info: Obtains __GENUS from API result		
Call WMI API	API Name: Win32_Processor::Get Args: (__PATH, 0, \\FIN-Adam-Serve\root\cimv2:Win32_Processor.DeviceID="CPU0", 8, 64) Return: 0	892	3112

Call WMI API	API Name: Win32_Processor::Get Args: (processorID, 0, 1, 8, 32) Return: 0	892	3112
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3112 Info: Obtains processorID from API result		
Call WMI API	API Name: Win32_Processor::Get Args: (processorID, 0, 1, 8, 32) Return: 0	892	3112
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5dec99ea-2cb6-4b5f-8ef9-a01742e42dc9 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 13cbd18, 6cef5b8) Return: 0	892	3112
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, , 80, , 0, 6cef5b8) Return: 0	892	3112
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\FIN-Adam-Serve\ROOT\cimv2:Win32_NetworkAdapterConfiguration, 8, 64) Return : 0	892	3112
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__CLASS, 0, Win32_NetworkAdapterConfiguration, 8, 64) Return: 0	892	3112
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	892	3112
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_69dcdbbc-7545-4a92-af9e-33f77c87b07f Type: VSDT_COM_DOS	892	824
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\FIN-Adam-Serve\root\cimv2:Win32_NetworkAdapterConfiguration.Index=0, 8, 64) Return: 0	892	3112
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	892	3112
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	892	3112
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	892	3112
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\FIN-Adam-Serve\root\cimv2:Win32_NetworkAdapterConfiguration.Index=1, 8, 64) Return: 0	892	3112
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, -1, 11, 0) Return: 0	892	3112
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a18a8c1a-12dc-421c-8600-4ee0bad81245 Type: VSDT_COM_DOS	892	824
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, -1, 11, 0) Return: 0	892	3112
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (MacAddress, 0, 00:1F:3C:8C:8D:BB, 8, 0) Return: 0	892	3112
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (MacAddress, 0, 00:1F:3C:8C:8D:BB, 8, 0) Return: 0	892	3112
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	892	3112
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\FIN-Adam-Serve\root\cimv2:Win32_NetworkAdapterConfiguration.Index=4, 8, 64) Return: 0	892	3112
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6056746f-5eb1-4f3a-a8df-0ddb84cd9be7 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_057949d9-f265-4ae0-bb39-c8d4b13ac0ab Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9230a1ef-a3a0-4cb5-8f95-eb099d42b1d8 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9a528d13-04a3-448c-b528-943230be3cac Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_35c6ed74-ae9b-4cf0-bc62-580ddbdf2b29 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4af5a9e0-e2c2-48b5-8b10-1958ba4a717f Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_decaba2c-dbc5-4d8d-a112-c9522a435438 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_86d0fa65-46e2-4936-892e-13d04a74cc24 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_450102ae-6106-4c4e-a008-ec847f4ec874 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7eb349f9-d8a6-4e3d-be7d-3dbe7de3205e Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_769f96d2-2c3a-4719-b9a6-63d1aa888a67 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7c0114f6-3a44-43d0-8833-ef686c9618ad Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_282c7b1d-8a86-4fe0-8862-782b1ea55447 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95c6c018-1eea-4287-a70c-7d305f80a176 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4778ef75-3dba-4959-a541-fe75d8a1069d Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824

Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_623a97e5-a4a4-466d-9768-cbb2f5fe0748 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_494b1a60-2944-4ad6-8ab2-f4d9be82a1c9 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9fc74e9c-4ec2-4a28-8c76-d95b3e56c98a Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_22a63118-307f-4f05-b4a2-542141f4fb64 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9d05625e-83a4-4a86-9f00-369a934ad822 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4b614778-91a7-4226-a3d3-8991c69c115f Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_063b6e0a-7fdb-43f9-a8db-574e0bb22440 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_516e6127-5e24-4897-9042-e754cba0eb55 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e2146bfe-39f2-4b5a-9190-3cbd628edc39 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7300dbec-2865-45cc-ac58-5c32edfef1f2 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_33bf3a44-1fc4-4e94-accd-a05eca95c165 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9c957b29-9561-45b4-9f5f-b844c5c1ce99 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0ded4e37-020f-4c61-ab7d-a992ac43dc33 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ea1f505a-a69a-40c3-a9cc-7b34489fd8b9 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5ab30fef-f01b-414b-979d-49e08404589f Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ec0b05e3-e8e6-4b86-a46d-76d9d8af06f4 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ed9f9ad6-da58-41ab-beda-681f9c66e286 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a5318292-bdf9-41a5-b065-da2980715f5e Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_62ed1c2b-d7bc-4888-9254-487fc55c4b4b Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2d9adf05-31af-4c86-8de0-26b3bbfcdcce Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a63c224e-fd93-4e45-bcd9-8ac0f6be3f74 Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_57a19812-ad31-47d3-b27b-900612eb602c Type: VSDT_COM_DOS	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	892	824
Add File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log Type: VSDT_ASCII	892	824
Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log Type: VSDT_ASCII	892	824
Detection	Threat Characteristic: Modifies configuration files to perform rogue functions File: %windir%\SYSTEM32\DRIVERS\ETC\HOSTS Modified Content: 127.0.0.1		
Write File	Path: %windir%\System32\drivers\etc\hosts Type: VSDT_ASCII	892	3112
Detection	Threat Characteristic: Modifies configuration files to perform rogue functions %windir%\System32\drivers\etc\hosts		
Detection	Threat Characteristic: Accesses decoy file %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data		
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\COMODO\ICEDRAGON\PROFILES.INI		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	892	3112

Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	892	3112
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Call System API	API Name: CLSIDFromProgIDEx Args: (WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8}) Return: 0	892	3112
Call System API	API Name: CLSIDFromProgIDEx Args: (WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8}) Return: 0	892	3112
Call System API	API Name: CLSIDFromProgIDEx Args: (WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8}) Return: 0	892	3112
Call System API	API Name: CLSIDFromProgIDEx Args: (WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8}) Return: 0	892	3112
Call System API	API Name: CLSIDFromProgIDEx Args: (WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8}) Return: 0	892	3112
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\FILEZILLA\RECENTSERVERS.XML		
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini		
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\key3.db		

▼ Screenshot



Process Graph Legend

Node

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

Notable Threat Characteristics

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