ID: 596584
Sample Name: Eset32.exe
Cookbook: default.jbs
Time: 22:08:24
Date: 24/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

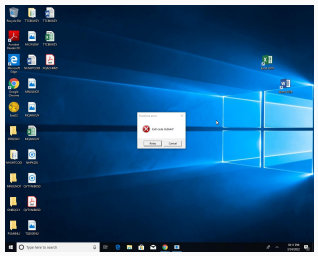
Windows Analysis Report

Eset32.exe

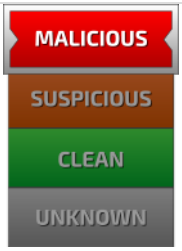
Overview

General Information

Sample Name:	Eset32.exe
Analysis ID:	596584
MD5:	b405bf6533c047..
SHA1:	bbb321d380c3f9..
SHA256:	5b35297b640271..
Tags:	exe
Infos:	



Detection



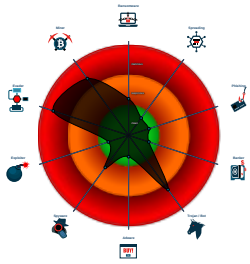
Xmrig

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Xmrig cryptocurrency…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Writes to foreign memory regions
- Found strings related to Crypto-Mini…
- .NET source code references suspic…
- Encrypted powershell cmdline option…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- May check the online IP address of…

Classification



Process Tree

- **System is w10x64**
- Eset32.exe (PID: 5096 cmdline: "C:\Users\user\Desktop\Eset32.exe" MD5: B405BF6533C047B1A47CECED3B42C23B)
  - 12.exe (PID: 5164 cmdline: C:\Users\user\AppData\Roaming\12.exe MD5: 7ADD9A3AB1734828F756F2725C452C9A)
    - cmd.exe (PID: 5336 cmdline: "cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 5668 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 2600 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" MD5: 95000560239032BC68B4C2FDFCDEF913)
      - powershell.exe (PID: 6332 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" MD5: 95000560239032BC68B4C2FDFCDEF913)
    - cmd.exe (PID: 4468 cmdline: cmd" /c schtasks /create /f /sc onlogon /rl highest /tn "System" /tr "C:\Users\user\AppData\Roaming\Windows\System.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 5408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 5720 cmdline: schtasks /create /f /sc onlogon /rl highest /tn "System" /tr "C:\Users\user\AppData\Roaming\Windows\System.exe" MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
    - cmd.exe (PID: 5464 cmdline: cmd" cmd /c "C:\Users\user\AppData\Roaming\Windows\System.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 6584 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - System.exe (PID: 4512 cmdline: C:\Users\user\AppData\Roaming\Windows\System.exe MD5: 7ADD9A3AB1734828F756F2725C452C9A)
        - cmd.exe (PID: 5924 cmdline: "cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
          - conhost.exe (PID: 4844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - powershell.exe (PID: 5832 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" MD5: 95000560239032BC68B4C2FDFCDEF913)
          - powershell.exe (PID: 6536 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" MD5: 95000560239032BC68B4C2FDFCDEF913)
        - sihost64.exe (PID: 6896 cmdline: "C:\Users\user\AppData\Roaming\Windows\Telemetry\sihost64.exe" MD5: E2DD8887AEE175EF9BEFD87B2F6105B3)
  - 1.exe (PID: 6656 cmdline: C:\Users\user\AppData\Roaming\1.exe MD5: D9F92868EEE8D3C8ECD29A7969419D29)
    - conhost.exe (PID: 6684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - AppLaunch.exe (PID: 5716 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)

- System.exe (PID: 3408 cmdline: C:\Users\user\AppData\Roaming\Windows\System.exe MD5: 7ADD9A3AB1734828F756F2725C452C9A)
  - cmd.exe (PID: 4812 cmdline: "cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQAgACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 6040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 6236 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" MD5: 95000560239032BC68B4C2FDFCDEF913)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000001A.00000002.701574814.00000000184D6000.00000004.00000800.00020000.00000000.sdmp	CoinMiner_Strings	Detects mining pool protocol string in Executable	Florian Roth	• 0x1c7e8:$sa1: stratum+tcp://
0000001A.00000002.701574814.00000000184D6000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
0000001A.00000002.701782612.0000000018691000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
Process Memory Space: System.exe PID: 4512	CoinMiner_Strings	Detects mining pool protocol string in Executable	Florian Roth	• 0x3cda8:$sa1: stratum+tcp:// • 0x40b9b:$sa1: stratum+tcp:// • 0x17c640:$sa1: stratum+tcp:// • 0x180425:$sa1: stratum+tcp://
Process Memory Space: System.exe PID: 4512	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
26.2.System.exe.18691d78.9.raw.unpack	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
26.2.System.exe.18691d78.9.unpack	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	

Sigma Signatures

There are no malicious signatures, click here to show all signatures.

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Bitcoin Miner

Yara detected Xmrig cryptocurrency miner

Found strings related to Crypto-Mining

Networking

May check the online IP address of the machine

Potential dropper URLs found in powershell memory

System Summary

PE file contains section with special chars

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

.NET source code references suspicious native API functions

Encrypted powershell cmdline option found

Allocates memory in foreign processes

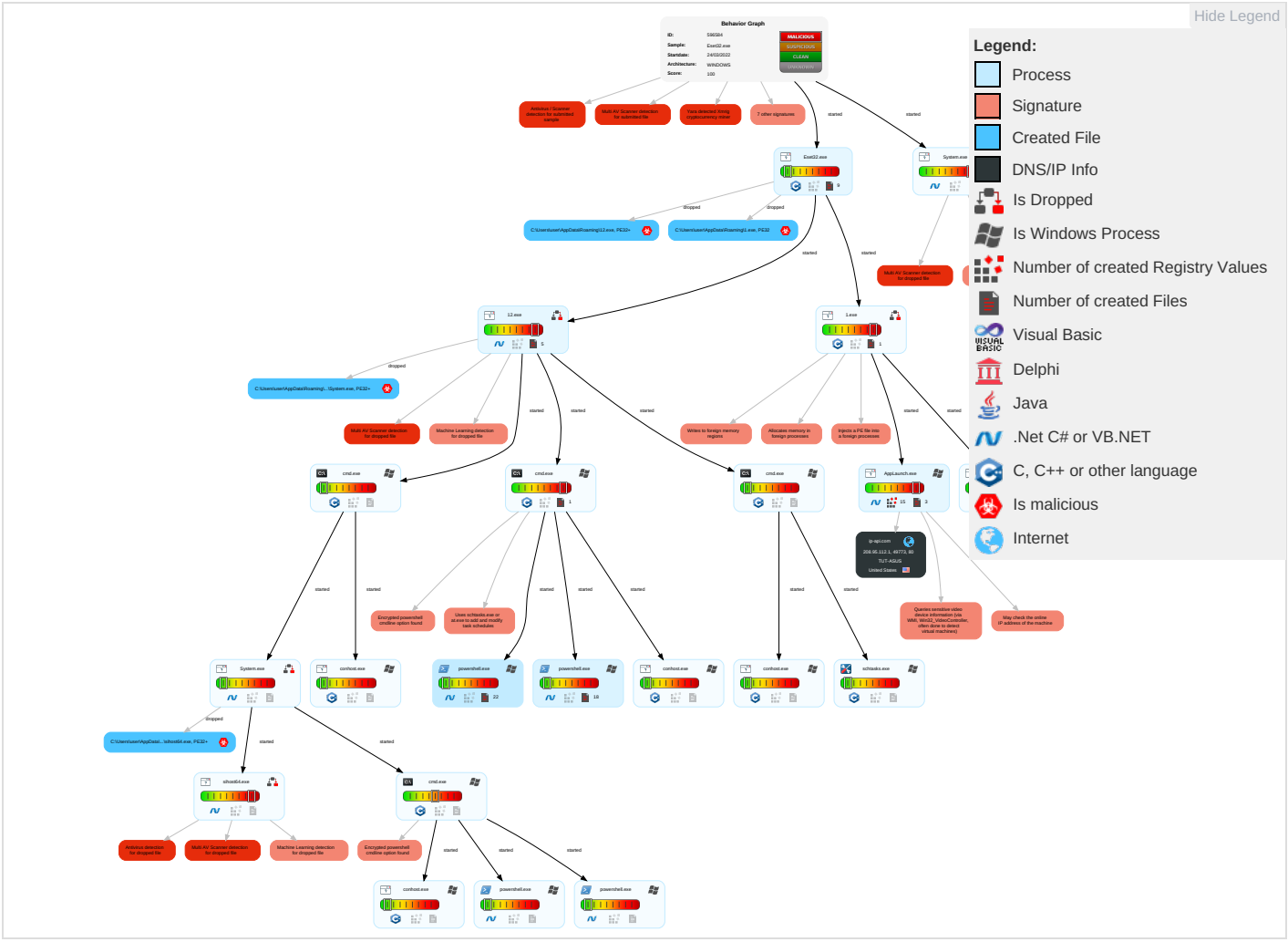
Injects a PE file into a foreign processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 Access Token Manipulation	1 Disable or Modify Tools	OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	3 1 1 Process Injection	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	1 Scheduled Task/Job	2 1 Obfuscated Files or Information	Security Account Manager	1 6 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Scheduled Task/Job	Logon Script (Mac)	Logon Script (Mac)	2 1 Software Packing	NTDS	1 Query Registry	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	1 PowerShell	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	2 1 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	1 3 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 1 1 Process Injection	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 System Network Configuration Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

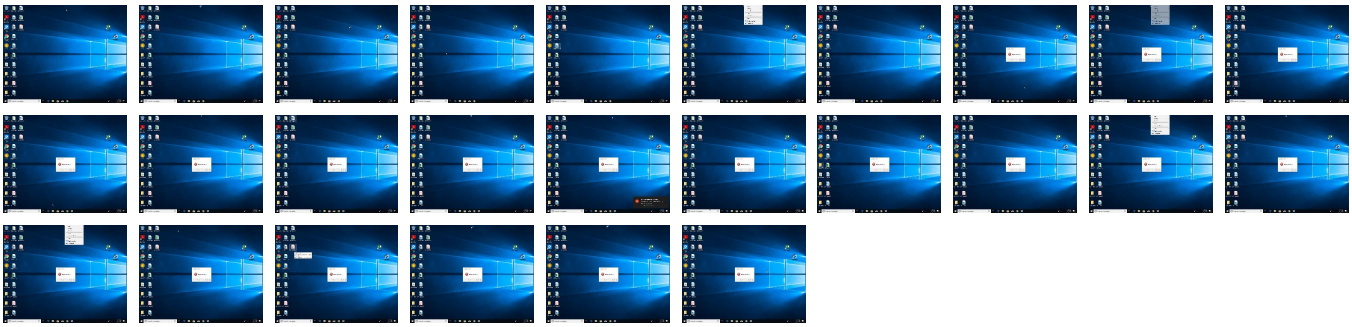
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Eset32.exe	63%	Virustotal		Browse
Eset32.exe	14%	Metadefender		Browse
Eset32.exe	60%	ReversingLabs	Win32.Trojan.Zenpak	
Eset32.exe	100%	Avira	HEUR/AGEN.1210313	
Eset32.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Windows\Telemetry\sihost64.exe	100%	Avira	HEUR/AGEN.1235806	
C:\Users\user\AppData\Roaming\Windows\Telemetry\sihost64.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\1.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\12.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Windows\System.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\1.exe	37%	Virustotal		Browse
C:\Users\user\AppData\Roaming\1.exe	45%	ReversingLabs	Win32.Trojan.Zenpak	
C:\Users\user\AppData\Roaming\12.exe	60%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\12.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.CoinminerX	
C:\Users\user\AppData\Roaming\Windows\System.exe	60%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Windows\System.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.CoinminerX	
C:\Users\user\AppData\Roaming\Windows\Telemetry\sihost64.exe	30%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Windows\Telemetry\sihost64.exe	73%	ReversingLabs	ByteCode-MSIL.Trojan.Tedy	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
36.0.sihost64.exe.fe0000.0.unpack	100%	Avira	HEUR/AGEN.1235806		Download File
6.2.AppLaunch.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1203048		Download File
1.2.12.exe.370000.0.unpack	100%	Avira	HEUR/AGEN.1221928		Download File
22.0.System.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1221928		Download File
0.0.Eset32.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
26.2.System.exe.d10000.0.unpack	100%	Avira	HEUR/AGEN.1221928		Download File
0.2.Eset32.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
26.0.System.exe.d10000.0.unpack	100%	Avira	HEUR/AGEN.1221928		Download File
1.0.12.exe.370000.0.unpack	100%	Avira	HEUR/AGEN.1221928		Download File
36.2.sihost64.exe.fe0000.0.unpack	100%	Avira	HEUR/AGEN.1235806		Download File
4.3.1.exe.2610000.0.unpack	100%	Avira	HEUR/AGEN.1203048		Download File
22.2.System.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1221928		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net02	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://https://pidgin.im0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crl.mi	0%	URL Reputation	safe	
http://ip-api.com4	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://www.jsonrpc.org/	0%	URL Reputation	safe	
http://crl.micros	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ip-api.com	208.95.112.1	true	false		high

Contacted URLs

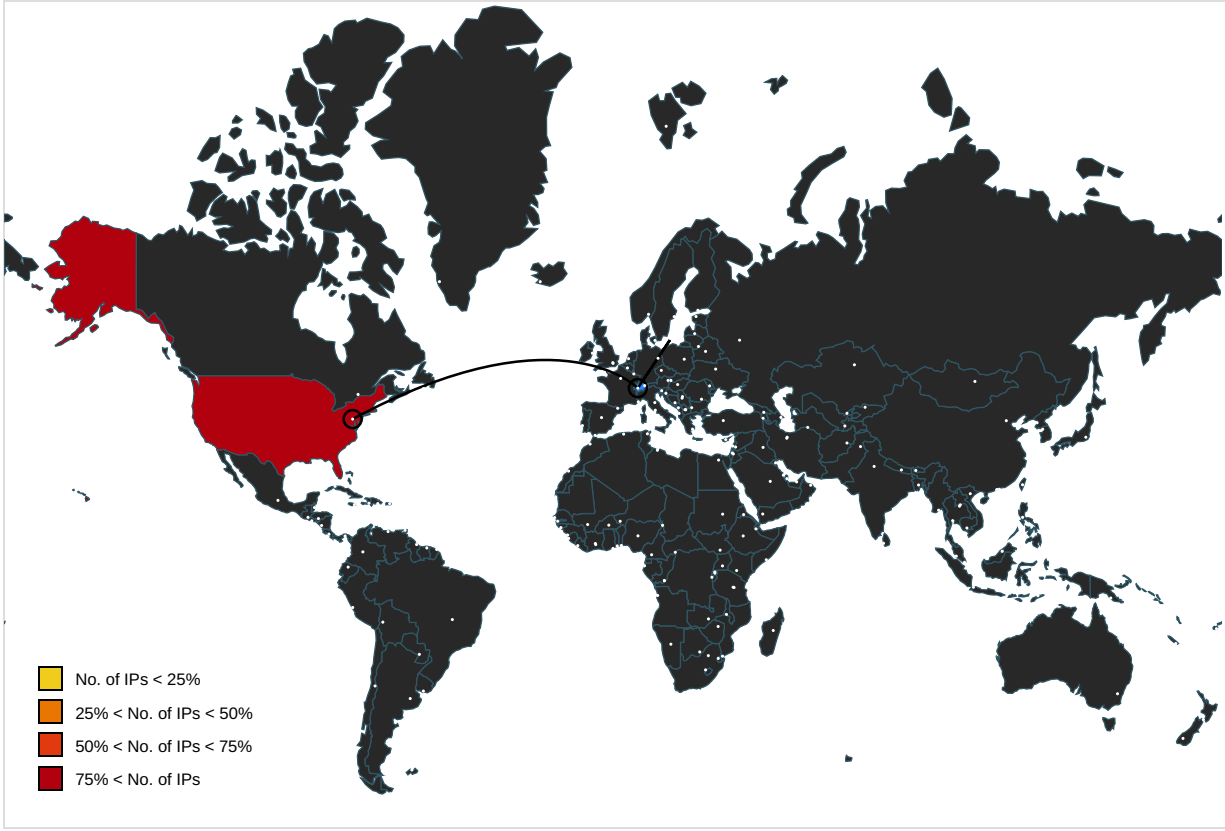
Name	Malicious	Antivirus Detection	Reputation
http://ip-api.com/line/?fields=hosting	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 0000000A.00000002.511738672.0000021AA3724000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0	Eset32.exe, 00000000.00000002.429962678.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.sectigo.com0	Eset32.exe, 00000000.00000002.429962678.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000000A.00000002.501780713.0000021A938D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 0000000A.00000002.501780713.0000021A938D0000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000001E.00000002.625526562.0000024F8D88F000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000021.00000002.681492895.000002BE88B10000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ocsp.entrust.net03	Eset32.exe, 00000000.00000002.429962678.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000000A.00000002.501780713.0000021A938D0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ocsp.entrust.net02	Eset32.exe, 00000000.00000002.429962678.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http://https://go.micro	powershell.exe, 0000000A.00000002.510560064.0000021A948A1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000A.00000002.511051451.0000021A94B38000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000A.00000002.511415597.0000021A94D18000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.entrust.net/rpa03	Eset32.exe, 00000000.00000002.429962678.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 0000000A.00000002.511738672.0000021AA3724000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 0000000A.00000002.511738672.0000021AA3724000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://aia.entrust.net/ts1-chain256.cer01	Eset32.exe, 00000000.00000002.429962678.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false		high
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	Eset32.exe, 00000000.00000002.429962678.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http://https://pidgin.im0	Eset32.exe, 00000000.00000002.429962678.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	Eset32.exe	false		high
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	Eset32.exe, 00000000.00000002.429962678.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/Pester/Pester	powershell.exe, 0000000A.00000002.501780713.0000021A938D0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/openwall/john/issues/3454#issuecomment-436899959	System.exe, 0000001A.00000002.701574814.00000000184D6000.00000004.00000800.00020000.00000000.sdmp, System.exe, 0000001A.00000002.701782612.0000000018691000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.mi	powershell.exe, 0000001E.00000002.634745548.0000024FA5AC0000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000021.00000002.678756357.000002BE86A75000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ip-api.com4	AppLaunch.exe, 00000006.00000002.708101051.0000000006BB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_Error	Eset32.exe	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 0000000A.00000002.501780713.0000021A938D0000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000001E.00000002.625526562.0000024F8D88F000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000021.00000002.681492895.000002BE88B10000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 0000000A.00000002.511738672.0000021AA3724000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 0000000A.00000002.511738672.0000021AA3724000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ip-api.com	AppLaunch.exe, 00000006.00000002.708101051.0000000006BB4000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000006.00000002.708582880.0000000006C17000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jsonrpc.org/	System.exe, 0000001A.00000002.701782612.0000000018691000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.codeplex.com/DotNetZip	AppLaunch.exe, 00000006.00000002.705990964.0000000000402000.00000020.00000400.00020000.00000000.sdmp	false		high
http://crl.entrust.net/ts1ca.crl0	Eset32.exe, 00000000.00000002.429962678.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	12.exe, 00000001.00000002.552111888.0000000003495000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000006.00000002.708101051.0000000006BB4000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000A.00000002.501374621.0000021A936C1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000001E.00000002.624837713.0000024F8D681000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000021.00000002.679354335.000002BE88901000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.entrust.net/rpa0	Eset32.exe, 00000000.00000002.429962678.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	Eset32.exe, 00000000.00000002.429962678.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false		high
http://crl.micros	powershell.exe, 00000021.00000002.678756357.000002BE86A75000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.gnu.org/licenses/	System.exe, 0000001A.00000002.701574814.00000000184D6000.00000004.00000800.00020000.00000000.sdmp, System.exe, 0000001A.00000002.701782612.0000000018691000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.95.112.1	ip-api.com	United States		53334	TUT-ASUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	596584
Start date and time:	2022-03-24 21:08:24 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Eset32.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	37
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.mine.winEXE@40/23@1/1
EGA Information:	• Successful, ratio: 33.3%
HDC Information:	• Successful, ratio: 15.9% (good quality ratio 15.3%) • Quality average: 83.3% • Quality standard deviation: 24.9%

HCA Information:	• Successful, ratio: 74% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.125.122.176, 20.54.89.106, 52.152.110.14, 20.54.110.249, 52.242.101.226
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Execution Graph export aborted for target 1.exe, PID 6656 because there are no executed function
- Execution Graph export aborted for target 12.exe, PID 5164 because it is empty
- Execution Graph export aborted for target System.exe, PID 3408 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 2600 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:09:51	API Interceptor	126x Sleep call for process: powershell.exe modified
22:10:22	API Interceptor	2x Sleep call for process: 12.exe modified
22:10:30	Task Scheduler	Run new task: System path: C:\Users\user\AppData\Roaming\Windows\System.exe
22:11:17	API Interceptor	1x Sleep call for process: System.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\12.exe.log	
Process:	C:\Users\user\AppData\Roaming\12.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	973
Entropy (8bit):	5.374440234733254
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPTxAIDAWDLI4MWuCWzAbDLI4MNCIBTa51KDLI4MN5P6D1Bakvoc:ML9E4KrVE4K5sXE4+21qE4GiD0E4KeGj
MD5:	55B1C358C76C36555547AB8BA39CB42E
SHA1:	63BD54BA7CB70FB481C8D625EBA24A5E2D6564F2
SHA-256:	33367C74DE2EC5A5DE6FDAD331DCBF09EB0C8EA333708F7CD3C0228D8A466240
SHA-512:	D33E61E1A6304955B413893AEC1C82A13F60D775888F47E74E37F747A63CF7FB6DDF2F9963157AC061845065E436AF4F677BC22EF5346E1FF1716FE5D0DB4A50
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..2,"System.IO.Compression, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\System.exe.log	
Process:	C:\Users\user\AppData\Roaming\Windows\System.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	973
Entropy (8bit):	5.374440234733254
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPTxAIDAWDLI4MWuCWzAbDLI4MNCIBTa51KDLI4MN5P6D1Bakvoc:ML9E4KrVE4K5sXE4+21qE4GiD0E4KeGj
MD5:	55B1C358C76C36555547AB8BA39CB42E
SHA1:	63BD54BA7CB70FB481C8D625EBA24A5E2D6564F2
SHA-256:	33367C74DE2EC5A5DE6FDAD331DCBF09EB0C8EA333708F7CD3C0228D8A466240
SHA-512:	D33E61E1A6304955B413893AEC1C82A13F60D775888F47E74E37F747A63CF7FB6DDF2F9963157AC061845065E436AF4F677BC22EF5346E1FF1716FE5D0DB4A50
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..2,"System.IO.Compression, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	18817
Entropy (8bit):	5.001217266823362
Encrypted:	false
SSDEEP:	384:sEvOjJiYoWVoGIpN6KQkj2dNXp5FOdBo+ib4+jjkjh4iUxL2c+4Jib4J:s0MiYoWV3IpNBQkj2dNZvOdBopj2h4iu
MD5:	A30A545B73C738B58F7D7089B1C9FF63
SHA1:	2F4784CFB523E34E6492F67EF7A04C7A20F16872
SHA-256:	2F1991061F8982C2AAB4D49CAF78BE84E1282EFED26BE6775989B0EC4C9464BC
SHA-512:	3C2DE1D82999C46EC2BA11DBA721E011950DC510F67E3226D61DF7CA9579F1F95F0BE7BE31A2BD61E92DDD1930563061131614C59D81472A92DBF529A114331
Malicious:	false
Reputation:	unknown
Preview:	PSMODULECACHE.....yH.8...I...C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....AfterEach.....Should.....BeforeEach.....Get-MockDynamicParameters.....It.....Assert-VerifiableMocks.....BeforeAll.....Context.....Set-TestInconclusive.....AfterAll.....Setup.....Set-DynamicParameterVariables.....Invoke-Pester.....Assert-MockCalled.....New-PesterOption.....I:]2...I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1.....Get-CIPolicyInfo.....Get-CIPolicyIdInfo.....Set-CIPolicySetting.....Merge-CIPolicy.....Edit-CIPolicyRule.....Set-CIPolicyVersion.....Set-CIPolicyIdInfo.....ConvertFrom-CIPolicy.....Set-HVCIOptions.....Add-SignerRule.....New-CIPolicy.....Get-SystemDriver.....Set-RuleOption.....Get-CIPolicy.....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1280
Entropy (8bit):	5.370793881110786
Encrypted:	false
SSDEEP:	24:3RPpQrLAo4KAxX5qRPD42HOoVZe9t4CvKaRSF8PJKnKwl9OVMn:hPerB4nqRL/Hvfe9t4CvpR48B47Hzn
MD5:	C670369412C03F8FA7DBD5472B975480
SHA1:	1EABE685DDD1AB29F6BC8CE34AD8C7E51CCC0E20
SHA-256:	EC2FED6FF59CE8D4D74B89B554CA364A470C45515C96D8C7E8FE76A0E5788BFB
SHA-512:	D9A64D79B98BC9B8B97B26422797BA97EA25CD23066349B51520E05A6F85F6033739A6B183CB3A45D416991AA1A6C9AEC184EE120C07732A364DFD0DD21D551
Malicious:	false
Reputation:	unknown
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Micro soft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q..... ...System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Tran sactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementT.....}0.2...K.....*.Mic rosoft.Management.Inf

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0yow3mvu.tj4.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1ylat3fg.wsq.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_44p5rcer.s4n.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_aimqagfl.k3o.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gq1rjo0b.xw4.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mcrj51io.qjc.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A

Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oy5qikcs.t2u.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qdo0e3x0.t1b.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_sb0bhm4m.q4d.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_st3h5wvp.0v4.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Roaming\1.exe

Process:	C:\Users\user\Desktop\Eset32.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4462384
Entropy (8bit):	5.902632936497891
Encrypted:	false
SSDEEP:	98304:4TrAyVoOVqO5uJFH6Ws49BRo0MWTNJH7apTgVijzPM/zyQIIU/jHwPe1mKJB:lyMFobXmijLczyYU7H5Z7
MD5:	D9F92868EEE8D3C8ECD29A7969419D29
SHA1:	0A74749DFCD4ECA403859431EBB18BA2A7E845BF
SHA-256:	B7154023E4778AC19EE6885BF403BF20CE675EF4B87F816E379FA98293526BE3
SHA-512:	5F29374B1BC47F8A978D03476BD8727DCB42B0D6AD028A6DECDBBF41363C70001EA017888B5E8A44326D86D2F2FDFE39ADE6C27861B7AA317F2F09A62BAE95F7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 45%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....0;b.....B..@.....B...@.....C.....C.<.....C.0I.....h.C.@.....B.\.....text...e?.....@..... ..`.QDwHSV..Q@..P...R@..D..... ..`.rdata..~.....B.....B.....@..@.data.....C.....C.....@....5{mr .....C.....C..... ..`.....

C:\Users\user\AppData\Roaming\12.exe

Process:	C:\Users\user\Desktop\Eset32.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2149888
Entropy (8bit):	**7.992953608237496**
Encrypted:	**true**
SSDEEP:	49152:+N1rE8yADMs6VVlywsIQH4V6Egj8ifqeuN9aDndygIRU:+ECDHWVlsZedgZfqeUChz
MD5:	7ADD9A3AB1734828F756F2725C452C9A
SHA1:	8EDE7005B99E59AF98DA451FBA6AFCE13F3A5629
SHA-256:	DAB7FDA27D80D645D5A709E59DD1AFE41A535885BC353C844077E570D051E763
SHA-512:	CD8582431009BA4B192D73E6E0494318D73E02993C9981C16F7481B30395F8DB9CDAF11B6D0D00AC487BE511CFFD5479FA70BCF5BB713CFAA7EDF7E8E876639
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 60%, Browse • Antivirus: ReversingLabs, Detection: 60%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....1;b.....".....@..... .....!.....@...@.....@..... ..H.....text..... .. ..rsrc..... ....@. .@.....H.....l4 .<.....;.....&...=W...#.".H..e._@....;.'z?.[sY... #)Lt...../2,.k..u..,W.m|..K.....,o...9G..Xt..'_.pN.3~.4...X.E....J6.[.,..r..wx.pE.....e..g...is.#.....l..E..F.f$1...."....f.-...yp.....(.%ns..?^tc.Yw.....%..t..rI.F..C.C"..j%.go$z.o.uAZ.....h.....s.0..W-Yf.....A.P.H]3.".sv....g.z.Q.S...l..55.`..w)c..Hx..;...t....a...J..l.(.T.4.;d...`..~..06T0.....c.".N.._.R..6.....U...4.....g7$?L/..W.kJ.

C:\Users\user\AppData\Roaming\Windows\System.exe

Process:	C:\Users\user\AppData\Roaming\12.exe

File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2149888
Entropy (8bit):	**7.992953608237496**
Encrypted:	**true**
SSDEEP:	49152:+N1rE8yADMs6VVlywsIQH4V6Egj8ifqeuN9aDndygIRU:+ECDHWVlsZedgZfqeUChz
MD5:	7ADD9A3AB1734828F756F2725C452C9A
SHA1:	8EDE7005B99E59AF98DA451FBA6AFCE13F3A5629
SHA-256:	DAB7FDA27D80D645D5A709E59DD1AFE41A535885BC353C844077E570D051E763
SHA-512:	CD8582431009BA4B192D73E6E0494318D73E02993C9981C16F7481B30395F8DB9CDAF11B6D0D00AC487BE511CFFD5479FA70BCF5BB713CFAA7EDF7E8E876639
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 60%, Browse • Antivirus: ReversingLabs, Detection: 60%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....1;b....."..... ....@..... .....!..... ..@...@.....@..... ....". ..H.....text..... .. ..`.rsrc..... ....@. .@.....H.....l4 .<.....;.....&...=W...#.".H..e._@....;.'z?.[sY... #)Lt...../2,.k..u..,W.m|..K.....,o...9G..Xt..'_.pN.3~.4...X.E.... J6.[..,..r..wx.pE.....e..g...is.#.....l..E..F.f$1...".....f.-...yp.....(.%ns..?^tc.Yw.....%..t..rl.F..C.C"..j%.go$z.o.uAZ.....h.....s.0..W-Yf.....A.P.H]3.".sv....g.z.Q.S...l..55.`..w)c..Hx. .;...t....a...J..l.(.T.4.;d...`..~..06T0.....c.".N.._.R..6.....U...4.....g7$?L/..W.kJ.

C:\Users\user\AppData\Roaming\Windows\Telemetry\sihost64.exe

Process:	C:\Users\user\AppData\Roaming\Windows\System.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	66560
Entropy (8bit):	5.675775271948851
Encrypted:	false
SSDEEP:	768:aQ//9WZSGIDUYU/+sdVaBk5EedlAiAJA1kt88ryseCmcgu+L5NtQEUF9zu1w13ue:JIZFIudWjtjOcfgpLpw13u9RGnlp3
MD5:	E2DD8887AEE175EF9BEFD87B2F6105B3
SHA1:	DFC0527E7425EF633DB3DB034E2E3DB8E09F9B28
SHA-256:	C09D1684236D9CE1D7E0C1C14119B4DC84CBC841DA4F4FB84131AA0F367F38F1
SHA-512:	2313792B160D1D6E28BC2CC2D45BA25773BD5CA1434026316181088C4385C9265922174D65DFAC377768024F67F7B9E4CB1B9B6A4FA08606324797E4E1F1E93F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 30%, Browse • Antivirus: ReversingLabs, Detection: 73%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...m1;b..... ....@..... .....@..... ..@...@.....@..... ....@..... ..H.....text..... ....`.rsrc...@.... ....@..@.....H.....0g.....n.....(....*...(0...*.0..... .....8.....E.....8...*.~....~<...(.....(..... ....(...:....& ....8.. .....E.....$...8....(.... ....(....:....& ....8.....& ....(....9....&8.....E.....*...8.....~>...(.... ....(....9....& ....8....:.. ....(....9....&8.....&.n..V.....0..... .....8.....E..... ....8....*.r...p.. /...8.....E1.....!...P....._...

C:\Users\user\Documents\20220324\PowerShell_transcript.841618.0_G0nLw0.20220324221054.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	6069
Entropy (8bit):	5.526227340041785
Encrypted:	false
SSDEEP:	96:BZZ/8N2cLqDo1ZJFZd/8N2cLqDo1ZA3x1xvxjZf/8N2cLqDo1ZFSx/x/xWeZ4H:lcdcic7fH
MD5:	2A07327783C8C059278FB8131A15BC86
SHA1:	72A793666AD245E17EE327066392AAB66F4A8578
SHA-256:	428716E884350ADB02D14DC21BF1832BE3CFFEADC03F91889BE8EAC50B8F822C
SHA-512:	9FC92E8F0D6D9CE6364F3C4CE486C15667856B01BC36C9630F6673E31012C2DFF60132AFA7EA813ED14031E602E9B24841755CC8F8299C4DD5CC163D094674C
Malicious:	false
Reputation:	unknown

Preview:	.**********..Windows PowerShell transcript start..Start time: 20220324221056..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 841618 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -EncodedCommand QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAG MAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6 AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA..Process ID: 6236..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..Serializati onVersion: 1.1.0.1..**********..**********..Command start time: 20220324221056..**********..PS>Add-MpPreference -ExclusionPath @($env: UserProfile,$env:SystemDrive) -Force..**********..Windows PowerShell transcript start..S

C:\Users\user\Documents\20220324\PowerShell_transcript.841618.3pgwcPiq.20220324221049.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	6069
Entropy (8bit):	5.524487604789142
Encrypted:	false
SSDEEP:	96:BZL/8N2cYqDo1ZDFZd/8N2cYqDo1Zo3x1xvxjZ4/8N2cYqDo1ZySx/x/xpZq:XcQcWcB
MD5:	F0330880F2F7BDF92334BE868A3E2B76
SHA1:	7FB360CC5173C1C87BA2A9D8B46733092212BE7D
SHA-256:	579A82C295646CF09AD1D49D893B5AE26584C825202E65337B29778D9CEAA73E
SHA-512:	3C8334679B855BD1B2893326322B7BEBFE3CE55DE0DBA67CDD9FB2C4CE26B119903017F81EB5FFDC6765DCAC3116181DFCC58E7BC5F775C56275B032C13BB 70
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220324221050..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 841618 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -EncodedCommand QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAG MAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6 AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA..Process ID: 5832..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..Serializati onVersion: 1.1.0.1..**********..**********..Command start time: 20220324221050..**********..PS>Add-MpPreference -ExclusionPath @($env: UserProfile,$env:SystemDrive) -Force..**********..Windows PowerShell transcript start..S

C:\Users\user\Documents\20220324\PowerShell_transcript.841618.C+N4AHXZ.20220324221113.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5764
Entropy (8bit):	5.524393941447013
Encrypted:	false
SSDEEP:	96:BZw/8N2AMiqDo1ZLZl/8N2AMiqDo1ZRgC4jZ9/8N2AMiqDo1ZSBoouZl:0tzW
MD5:	FD595612596392EF16B26200199439F4
SHA1:	06112F5363BFC9E636106AE33A263079CA122830
SHA-256:	7495F81371E9D6D4316B38A94A66D63597C21ED48170B36D87E2643086D6528F
SHA-512:	FD3CD847DACE784FBEB6C2680CC9543100DDC8E855394A80A1FB6D31ADF9D3FAE1FDBA3FE4043CEF98318AA2BED01B61037ABFDB6443E40BA5DDA878B5B0 DBC8
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220324221114..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 841618 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -EncodedCommand QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAG MAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwBy AGMAZQA=..Process ID: 6536..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1.. CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..********** **..Command start time: 20220324221114..**********..PS>Add-MpPreference -ExclusionExtension @('exe','dll') -Force..**********..Windows P owerShell transcript start..Start time: 20220324221231..Username: computer\user..

C:\Users\user\Documents\20220324\PowerShell_transcript.841618.LAWMVj_f.20220324221018.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5764
Entropy (8bit):	5.522947101485942
Encrypted:	false
SSDEEP:	96:BZI/8N2AM2tqDo1ZbZY/8N2AM2tqDo1Z8gC4jZ2/8N2AM2tqDo1ZUBooOZR:E/t+
MD5:	75A1F14AC41D6806DAA818318C905D78
SHA1:	BC191AECDC22CA7B0EA9EDCE1C630EA0413F03A1
SHA-256:	469CD3329590793020ED92B36F3B62FEDCDB0C4281DB636C0FF0D31FFEC0EFEF

SHA-512:	D742DBE9478175D35AEF470C444631E8BBDF83AAE27DF0B297B611856FB77FF6C0301B0D48068C71BDFFA47853B79EA61DFA1DBB5BFA371D62F1973ACB651947
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220324221019..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 841618 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -EncodedCommand QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=..Process ID: 6332..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..********** **..Command start time: 20220324221019..**********..PS>Add-MpPreference -ExclusionExtension @('exe','dll') -Force..**********..Windows PowerShell transcript start..Start time: 20220324221136..Username: computer\user..

C:\Users\user\Documents\20220324\PowerShell_transcript.841618.sZdefLPX.20220324220950.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	6069
Entropy (8bit):	5.525103873550551
Encrypted:	false
SSDEEP:	96:BZa/8N2c4qDo1ZqLFZUm/8N2c4qDo1Zr3x1xvxjZl/8N2c4qDo1Z7Sx/x/xCZJ:OcNAOcmcY
MD5:	96B72526B59BA604F3C8CEB114B96D15
SHA1:	DAA9D1365D4766A78CB16003EFDE94D9E9B8F786
SHA-256:	E58278B16390EA93E36F7E0769530BB23666CBC8946916A3F0E2B768CBAE9C1A
SHA-512:	84AAFCA8526DC56CEDCC2466DD7AAF9FCA9D8F4755B2D63009962EF803DC0ACFE30FC40617D0A3018DB20CF43A843D3F1022D8700A0B47DA93A228E94A304B8
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220324220951..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 841618 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -EncodedCommand QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA..Process ID: 2600..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220324220951..**********..PS>Add-MpPreference -ExclusionPath @($env:UserProfile,$env:SystemDrive) -Force..**********..Windows PowerShell transcript start..S

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.986911660203424
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Eset32.exe
File size:	4139932
MD5:	b405bf6533c047b1a47ceced3b42c23b
SHA1:	bbb321d380c3f9d17e49a9f2167234742e292e4d
SHA256:	5b35297b640271fea6e846f28d07852589f60ab88ee597c0e2eea68a5de3bec9
SHA512:	662af21fa3c267ca3a7b451d1a969e1b2dc4fd197368a066e7273b51673bf6def91b02b4d5e429c3b6947a5c97ceb17703b0e716eb6e6dc5a146ca2af40a4c82
SSDEEP:	98304:52NBK/xafUdOXhsemQTJSDVnAjKU4trvh9L9mxSSKKE:KU48cXhsehTEVnPBo/E
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L...".$_.....f...|.....H3.....@

File Icon

Icon Hash:	70f0ca9692f2f071

Static PE Info

General

Entrypoint:	0x403348
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D722 [Sat Aug 1 02:44:50 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	ced282d9b261d1462772017fe2f6972b

Authenticode Signature	
Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview
Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B8h]
call dword ptr [004080BCh]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F42Ch], eax
je 00007F0995393483h
push ebx
call 00007F09953965E6h
cmp eax, ebx
je 00007F0995393479h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F0995396562h
push esi
call dword ptr [004080CCh]

Instruction
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F099539345Dh
push 0000000Bh
call 00007F09953965BAh
push 00000009h
call 00007F09953965B3h
push 00000007h
mov dword ptr [0042F424h], eax
call 00007F09953965A7h
cmp eax, ebx
je 00007F0995393481h
push 0000001Eh
call eax
test eax, eax
je 00007F0995393479h
or byte ptr [0042F42Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F4F8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429850h
call dword ptr [0040816Ch]
push 0040A188h

Rich Headers	
Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x10fa0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3f099c	0x2200	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6457	0x6600	False	0.66823682598	data	6.43498570321	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x8000	0x1380	0x1400	False	0.4625	data	5.26100389731	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25538	0x600	False	0.463541666667	data	4.133728555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x10fa0	0x11000	False	0.147073184743	data	3.75019672411	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x38190	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_DIALOG	0x489b8	0x100	data	English	United States
RT_DIALOG	0x48ab8	0x11c	data	English	United States
RT_DIALOG	0x48bd8	0x60	data	English	United States
RT_GROUP_ICON	0x48c38	0x14	data	English	United States
RT_MANIFEST	0x48c50	0x34b	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

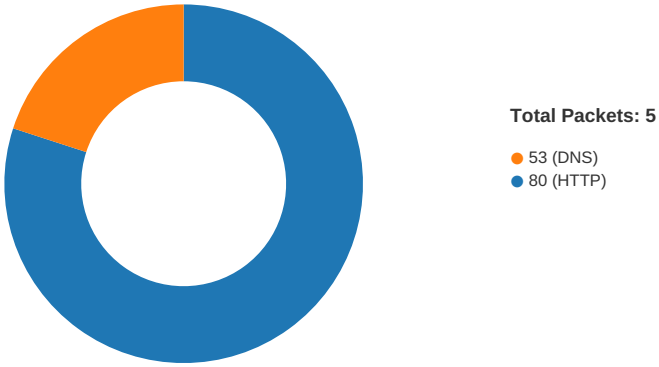
DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, ReadFile, GetTempFileNameA, WriteFile, RemoveDirectoryA, CreateProcessA, CreateFileA, GetLastError, CreateThread, CreateDirectoryA, GlobalUnlock, GetDiskFreeSpaceA, GlobalLock, SetErrorMode, GetVersion, lstrcpynA, GetCommandLineA, GetTempPathA, lstrlenA, SetEnvironmentVariableA, ExitProcess, GetWindowsDirectoryA, GetCurrentProcess, GetModuleFileNameA, CopyFileA, GetTickCount, Sleep, GetFileSize, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 24, 2022 22:09:52.593719006 CET	49773	80	192.168.2.5	208.95.112.1
Mar 24, 2022 22:09:52.623347998 CET	80	49773	208.95.112.1	192.168.2.5
Mar 24, 2022 22:09:52.623478889 CET	49773	80	192.168.2.5	208.95.112.1
Mar 24, 2022 22:09:52.624797106 CET	49773	80	192.168.2.5	208.95.112.1
Mar 24, 2022 22:09:52.654623985 CET	80	49773	208.95.112.1	192.168.2.5
Mar 24, 2022 22:09:52.758847952 CET	49773	80	192.168.2.5	208.95.112.1
Mar 24, 2022 22:10:23.416403055 CET	80	49773	208.95.112.1	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 24, 2022 22:09:52.541419029 CET	63712	53	192.168.2.5	8.8.8.8
Mar 24, 2022 22:09:52.572071075 CET	53	63712	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 24, 2022 22:09:52.541419029 CET	192.168.2.5	8.8.8.8	0xe21d	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 24, 2022 22:09:52.572071075 CET	8.8.8.8	192.168.2.5	0xe21d	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ip-api.com

HTTP Packets

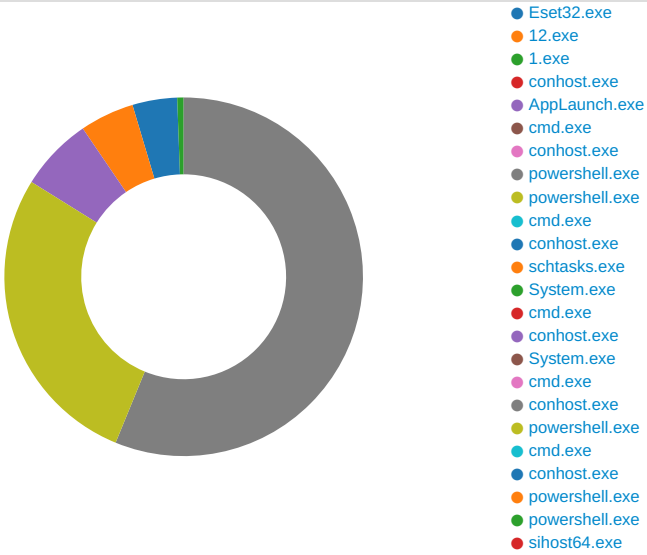
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49773	208.95.112.1	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
Mar 24, 2022 22:09:52.624797106 CET	935	OUT	GET /line/?fields=hosting HTTP/1.1 Host: ip-api.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Mar 24, 2022 22:09:52.654623985 CET	935	IN	HTTP/1.1 200 OK Date: Thu, 24 Mar 2022 21:09:51 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 5 Access-Control-Allow-Origin: * X-Ttl: 60 X-Rl: 44 Data Raw: 74 72 75 65 0a Data Ascii: true

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Eset32.exe PID: **5096**, Parent PID: **3420**

General

Target ID:	0
Start time:	22:09:31
Start date:	24/03/2022
Path:	C:\Users\user\Desktop\Eset32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Eset32.exe"
Imagebase:	0x400000
File size:	4139932 bytes
MD5 hash:	B405BF6533C047B1A47CECED3B42C23B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: 12.exe PID: **5164**, Parent PID: **5096**

General

Target ID:	1
Start time:	22:09:32
Start date:	24/03/2022
Path:	C:\Users\user\AppData\Roaming\12.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\12.exe
Imagebase:	0x370000
File size:	2149888 bytes
MD5 hash:	7ADD9A3AB1734828F756F2725C452C9A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 60%, Virustotal, Browse • Detection: 60%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA5016F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA5016F1E9	unknown
C:\Users\user\AppData\Roaming\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA4BF4F35D	CreateDirectoryW
C:\Users\user\AppData\Roaming\Windows\System.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FFA4C62817A	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\12.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA505D86ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Windows\System.exe	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 02 00 fd 31 3b 62 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0b 00 00 fd 20 00 00 06 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 40 01 00 00 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 21 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd1;b" @ !@@ @	success or wait	5	7FFA4C62817A	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\12.exe.log	0	973	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 49 4f 2e 43 6f 6d 70 72 65 73 73 69 6f 6e 2c 20 56 65 72	1,"fusion","GAC",01,"WinRT","N otApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\ Windows\assembly\NativeImages_ v4.0.30319_64\System\10a171391 82a9efd561f01fada9688a5\System .ni.dll",02,"System.IO.Compression, Ver	success or wait	1	7FFA505D8769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50042625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFA501112E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA5003B9DD	unknown

Analysis Process: 1.exe PID: **6656**, Parent PID: **5096**

General

Target ID:	4
Start time:	22:09:34
Start date:	24/03/2022
Path:	C:\Users\user\AppData\Roaming\1.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\1.exe
Imagebase:	0x400000
File size:	4462384 bytes
MD5 hash:	D9F92868EEE8D3C8ECD29A7969419D29
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 37%, Virustotal, Browse • Detection: 45%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	90			invalid handle	43	419000	WriteFile
unknown	unknown	1			invalid handle	5	419000	WriteFile

Analysis Process: conhost.exe PID: **6684**, Parent PID: **6656**

General

Target ID:	5
Start time:	22:09:36
Start date:	24/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AppLaunch.exe PID: **5716**, Parent PID: **6656**

General

Target ID:	6
Start time:	22:09:37
Start date:	24/03/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0x880000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E6FCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E6FCF06	unknown
C:\Users\user\AppData\Local\11e3ca1cc2de1e4f8cc2efe1558aa686	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6994BEFF	CreateDirectoryW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6E6D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6E6D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E6D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E6D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E6303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6E6DCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6E6DCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E6DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E6303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E6303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6E6D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6E6D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E6D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E6D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E6303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E6303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	69941B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	69941B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	69941B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	69941B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **5336**, Parent PID: **5164**

General

Target ID:	8
Start time:	22:09:44
Start date:	24/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQAgACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5668**, Parent PID: **5336**

General

Target ID:	9
Start time:	22:09:45
Start date:	24/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **2600**, Parent PID: **5336**

General

Target ID:	10
Start time:	22:09:46
Start date:	24/03/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA"
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA5016F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA5016F1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_aimqagfl.k3o.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4BF46FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qdo0e3x0.t1b.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4BF46FDD	CreateFileW
C:\Users\user\Documents\20220324	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA4BF4F35D	CreateDirectoryW
C:\Users\user\Documents\20220324\PowerShell_transcript.841618.sZdefLPX.20220324220950.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4BF46FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	7FFA48D603FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	7FFA48D603FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA48D603FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA48D603FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	7FFA48D603FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	7	7FFA48D603FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA48D603FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA48D603FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_aimqagfl.k3o.ps1	success or wait	1	7FFA4BF4F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qdo0e3x0.t1b.psm1	success or wait	1	7FFA4BF4F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_aimqagfl.k3o.ps1	0	1	31	1	success or wait	1	7FFA4BF4B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qdo0e3x0.t1b.psm1	0	1	31	1	success or wait	1	7FFA4BF4B526	WriteFile
C:\Users\user\Documents\20220324\PowerShell_transcript.841618.sZdefLPX.20220324220950.txt	0	3	ff		success or wait	1	7FFA4BF4B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220324\PowerShell_transcript.841618.sZdefLPX.20220324220950.txt	3	771	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 33 32 34 32 32 30 39 35 31 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 34 31 36 31 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77	********************Windows PowerShell transcript startStart time: 20220324220951Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 841618 (Microsoft Windows NT 10.0.17134.0)Host Application: pow	success or wait	44	7FFA4BF4B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 1b 00 00 00 79 48 fd 38 9f fd 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 64 31 17 00 00 00 08 00 00 00 44 65 73 63 72 69 62 65 02 00 00 00 11 00 00 00 47 65 74 2d 54 65 73 74 44 72 69 76 65 49 74 65 6d 02 00 00 00 0b 00 00 00 4e 65 77 2d 46 69 78 74 75 72 65 02 00 00 00 02 00 00 00 49 6e 02 00 00 00 0b 00 00 00 49 6e 76 6f 6b 65 2d 4d 6f 63 6b 02 00 00 00 0d 00 00 00 49 6e 4d 6f 64 75 6c 65 53 63 6f 70 65 02 00 00 00 04 00 00 00 4d 6f 63 6b 02 00 00 00 0e 00 00 00 53 61 66 65 47 65 74 43 6f 6d 6d 61 6e 64 02 00 00 00 09 00 00 00	PSMODULECACHEyH8lC:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1DescribeGet-TestDriveItemNew-FixtureInInvoke-MockInModuleScopeMockSafeGetCommand	success or wait	1	7FFA4BF4B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	00 00 00 03 00 00 00 67 63 62 01 00 00 00 0f 00 00 00 53 75 73 70 65 6e 64 2d 53 65 72 76 69 63 65 08 00 00 00 0d 00 00 00 53 74 6f 70 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0f 00 00 00 52 65 6e 61 6d 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 13 00 00 00 43 68 65 63 6b 70 6f 69 6e 74 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0a 00 00 00 53 70 6c 69 74 2d 50 61 74 68 08 00 00 00 0d 00 00 00 53 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 0b 00 00 00 47 65 74 2d 53 65 72 76 69 63 65 08 00 00 00 0c 00 00 00 53 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 50 6f 70 2d 4c 6f 63 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 47 65 74 2d 43 6c 69 70 62 6f 61 72 64 08 00 00 00 0c 00 00 00 53	gcbSuspend-ServiceStop-ComputerRename-ComputerCheckpoint-ComputerSplit-PathStart-ServiceGet-ServiceSet-TimeZoneRemove-ComputerPop-LocationGet-ClipboardS	success or wait	2	7FFA4BF4B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	4096	73 08 00 00 00 04 00 00 00 67 63 6c 73 01 00 00 00 12 00 00 00 49 6d 70 6f 72 74 2d 42 69 6e 61 72 79 4d 69 4c 6f 67 08 00 00 00 04 00 00 00 67 63 69 6d 01 00 00 00 04 00 00 00 72 63 69 6d 01 00 00 00 14 00 00 00 4e 65 77 2d 43 69 6d 53 65 73 73 69 6f 6e 4f 70 74 69 6f 6e 08 00 00 00 04 00 00 00 72 63 6d 73 01 00 00 00 04 00 00 00 73 63 69 6d 01 00 00 00 04 00 00 00 72 63 69 65 01 00 00 00 12 00 00 00 52 65 6d 6f 76 65 2d 43 69 6d 49 6e 73 74 61 6e 63 65 08 00 00 00 04 00 00 00 67 63 6d 73 01 00 00 00 0f 00 00 00 4e 65 77 2d 43 69 6d 49 6e 73 74 61 6e 63 65 08 00 00 00 0f 00 00 00 53 65 74 2d 43 69 6d 49 6e 73 74 61 6e 63 65 08 00 00 00 1b 00 00 00 52 65 67 69 73 74 65 72 2d 43 69 6d 49 6e 64 69 63 61 74 69 6f 6e 45 76 65 6e 74 08 00 00 00 19 00 00 00 47	sgclsImport-BinaryMiLoggcimrcimNew-CimSessionOptionrcmsscimrcieRemove-CimInstancegcmsNew-CimInstanceSet-CimInstanceRegister-CimIndicationEventG	success or wait	1	7FFA4BF4B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	16384	2433	63 6b 02 00 00 00 0e 00 00 00 53 61 66 65 47 65 74 43 6f 6d 6d 61 6e 64 02 00 00 00 09 00 00 00 41 66 74 65 72 45 61 63 68 02 00 00 00 06 00 00 00 53 68 6f 75 6c 64 02 00 00 00 0a 00 00 00 42 65 66 6f 72 65 45 61 63 68 02 00 00 00 19 00 00 00 47 65 74 2d 4d 6f 63 6b 44 79 6e 61 6d 69 63 50 61 72 61 6d 65 74 65 72 73 02 00 00 00 02 00 00 00 49 74 02 00 00 00 16 00 00 00 41 73 73 65 72 74 2d 56 65 72 69 66 69 61 62 6c 65 4d 6f 63 6b 73 02 00 00 00 09 00 00 00 42 65 66 6f 72 65 41 6c 6c 02 00 00 00 14 00 00 00 53 65 74 2d 54 65 73 74 49 6e 63 6f 6e 63 6c 75 73 69 76 65 02 00 00 00 07 00 00 00 43 6f 6e 74 65 78 74 02 00 00 00 08 00 00 00 41 66 74 65 72 41 6c 6c 02 00 00 00 1d 00 00 00 53 65 74 2d 44 79 6e 61 6d 69 63 50 61 72 61 6d 65 74 65 72 56 61 72 69 61	ckSafeGetCommandAfterEachShouldBeforeEachGet-MockDynamicParametersItAssert-VerifiableMocksBeforeAllSet-TestInconclusiveContextAfterAllSet-DynamicParameterVaria	success or wait	1	7FFA4BF4B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 09 00 00 00 12 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 0a 00 fd 04 1a 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFA5058F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 fd 27 fd fd 11 e3 4c fd fd 7d 19 b2 0b fd 09 00 00 00 0e 00 0f 00	8'L}	success or wait	17	7FFA5058F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	17	7FFA5058F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	11	7FFA5058F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	70 00 00 03	p	success or wait	1	7FFA5058F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	120	01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 00 0e fd 00 09 0e fd 00 0a 0e fd 00 0b 0e fd 00 0c 0e fd 00 0d 0e fd 00 0e 0e fd 00 0f 0c fd 00 10 0c fd 00 22 00 40 00 24 00 40 00 6a 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 18 00 40 00 57 00 40 00 0f 0e fd 00	"@$@j@@@@@@W@	success or wait	1	7FFA5058F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA5003B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50042625	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50042625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50042625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA5003B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA5003B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA5003B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA500262DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23112	success or wait	1	7FFA500263B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA501112E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFA4BF4B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	136	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFA501112E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA5003B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA5003B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFA4BF4B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	72	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	7FFA4BF4B526	ReadFile

Analysis Process: powershell.exe PID: **6332**, Parent PID: **5336**

General

Target ID:	16
Start time:	22:10:17
Start date:	24/03/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA="
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA5016F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA5016F1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gq1rjo0b.xw4.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4BF46FDD	CreateFileW
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_44p5rcer.s4n.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4BF46FDD	CreateFileW
C:\Users\user\Documents\20220324\PowerShell_transcript.841618.LAWMVj_f.20220324221018.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4BF46FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	7FFA48D603FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	7FFA48D603FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA48D603FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA48D603FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gq1rjo0b.xw4.ps1	success or wait	1	7FFA4BF4F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_44p5rcer.s4n.psm1	success or wait	1	7FFA4BF4F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gq1rjo0b.xw4.ps1	0	1	31	1	success or wait	1	7FFA4BF4B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_44p5rcer.s4n.psm1	0	1	31	1	success or wait	1	7FFA4BF4B526	WriteFile
C:\Users\user\Documents\20220324\PowerShell_transcript.841618.LAWMVj_f.20220324221018.txt	0	3	ff		success or wait	1	7FFA4BF4B526	WriteFile
C:\Users\user\Documents\20220324\PowerShell_transcript.841618.LAWMVj_f.20220324221018.txt	3	727	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 33 32 34 32 32 31 30 31 39 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 34 31 36 31 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77	**********Windows PowerShell transcript startStart time: 20220324221019Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 841618 (Microsoft Windows NT 10.0.17134.0)Host Application: pow	success or wait	44	7FFA4BF4B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 09 00 00 00 12 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 0a 00 fd 04 1a 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFA5058F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 fd 27 fd fd 11 e3 4c fd fd 7d 19 b2 0b fd 09 00 00 00 0e 00 0f 00	8'L}	success or wait	17	7FFA5058F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	17	7FFA5058F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	11	7FFA5058F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	70 00 00 03	p	success or wait	1	7FFA5058F6E8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	108	01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 00 0e fd 00 09 0e fd 00 0a 0e fd 00 0b 0e fd 00 0c 0e fd 00 0d 0e fd 00 0e 0e fd 00 0f 0c fd 00 10 0c fd 00 22 00 40 00 24 00 40 00 6a 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 18 00 40 00 57 00 40 00 0f 0e fd 00	"@$@j@@@@@@W@	success or wait	1	7FFA5058F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA5003B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50042625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50042625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50042625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA5003B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA5003B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA5003B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA5003B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA500262DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1228	success or wait	1	7FFA500263B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA501112E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3	success or wait	2	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	11	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	7FFA4BF4B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	2	7FFA4BF4B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA501112E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA501112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	15	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	7FFA4BF4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	2	7FFA4BF4B526	ReadFile

Analysis Process: cmd.exe PID: **4468**, Parent PID: **5164**

General

Target ID:	18
Start time:	22:10:28
Start date:	24/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd" /c schtasks /create /f /sc onlogon /rl highest /tn "System" /tr "C:\Users\user\AppData\Roaming\Windows\System.exe
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **5408**, Parent PID: **4468**

General

Target ID:	19
Start time:	22:10:28
Start date:	24/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **5720**, Parent PID: **4468**

General

Target ID:	20
Start time:	22:10:29
Start date:	24/03/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /create /f /sc onlogon /rl highest /tn "System" /tr "C:\Users\user\AppData\Roaming\Windows\System.exe"
Imagebase:	0x7ff69c230000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: System.exe PID: **3408**, Parent PID: **1040**

General

Target ID:	22
Start time:	22:10:30
Start date:	24/03/2022
Path:	C:\Users\user\AppData\Roaming\Windows\System.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Windows\System.exe
Imagebase:	0x1c0000
File size:	2149888 bytes
MD5 hash:	7ADD9A3AB1734828F756F2725C452C9A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 60%, Virustotal, Browse • Detection: 60%, ReversingLabs

Analysis Process: cmd.exe PID: **5464**, Parent PID: **5164**

General

Target ID:	23
Start time:	22:10:31
Start date:	24/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd" cmd /c "C:\Users\user\AppData\Roaming\Windows\System.exe
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6584**, Parent PID: **5464**

General

Target ID:	24
Start time:	22:10:32
Start date:	24/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: System.exe PID: **4512**, Parent PID: **5464**

General	
Target ID:	26
Start time:	22:10:32
Start date:	24/03/2022
Path:	C:\Users\user\AppData\Roaming\Windows\System.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Windows\System.exe
Imagebase:	0xd10000
File size:	2149888 bytes
MD5 hash:	7ADD9A3AB1734828F756F2725C452C9A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 0000001A.00000002.701574814.00000000184D6000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001A.00000002.701574814.00000000184D6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001A.00000002.701782612.0000000018691000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: **5924**, Parent PID: **4512**

General	
Target ID:	28
Start time:	22:10:47
Start date:	24/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQAgACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4844**, Parent PID: **5924**

General	
Target ID:	29
Start time:	22:10:48
Start date:	24/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **5832**, Parent PID: **5924**

General	
Target ID:	30
Start time:	22:10:48
Start date:	24/03/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA"
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cmd.exe PID: **4812**, Parent PID: **3408**

General	
Target ID:	31
Start time:	22:10:51
Start date:	24/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6040**, Parent PID: **4812**

General	
Target ID:	32
Start time:	22:10:52
Start date:	24/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **6236**, Parent PID: **4812**

General	
Target ID:	33
Start time:	22:10:53
Start date:	24/03/2022

Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA"
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: **6536**, Parent PID: **5924**

General	
Target ID:	35
Start time:	22:11:13
Start date:	24/03/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sihost64.exe PID: **6896**, Parent PID: **4512**

General	
Target ID:	36
Start time:	22:11:26
Start date:	24/03/2022
Path:	C:\Users\user\AppData\Roaming\Windows\Telemetry\sihost64.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\Windows\Telemetry\sihost64.exe"
Imagebase:	0xfe0000
File size:	66560 bytes
MD5 hash:	E2DD8887AEE175EF9BEFD87B2F6105B3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 30%, Virustotal, Browse • Detection: 73%, ReversingLabs

Disassembly

No disassembly