



Ahmad Rashid 2022677

Aizaz 2022078

Digital Forensics Project

“Windows malware analysis”

1. Introduction:

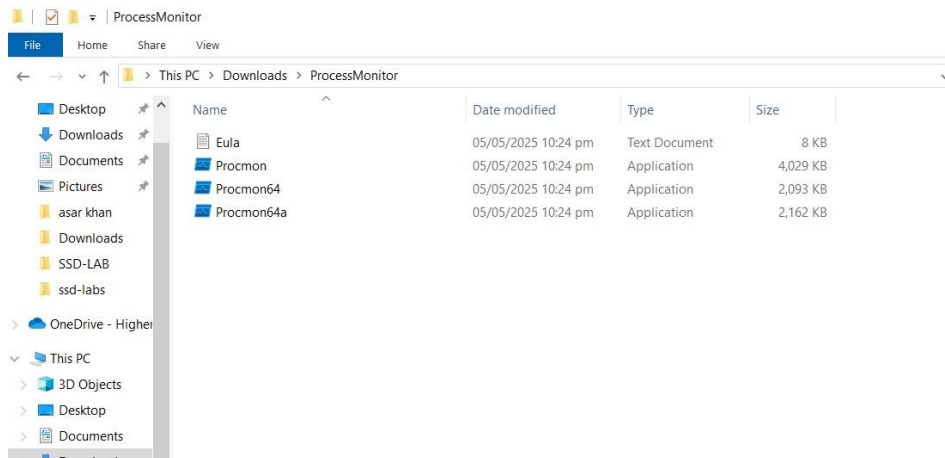
This project demonstrates step-by-step malware analysis conducted on a Windows system. Malware analysis is a crucial part of digital forensics to understand malicious behavior, detect indicators of compromise (IOCs), and strengthen system defenses.

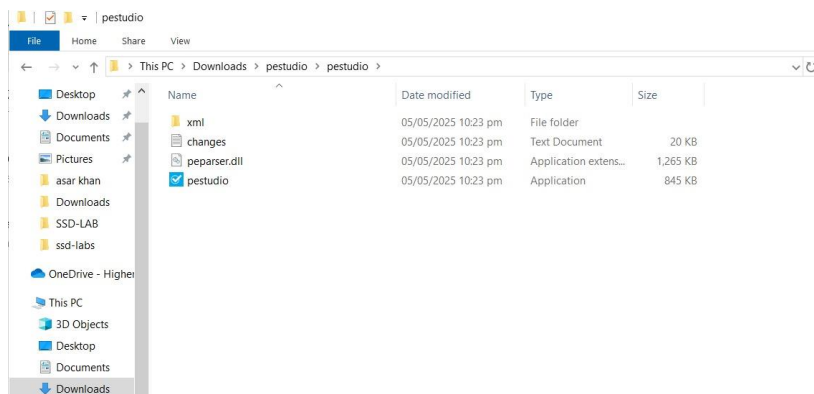
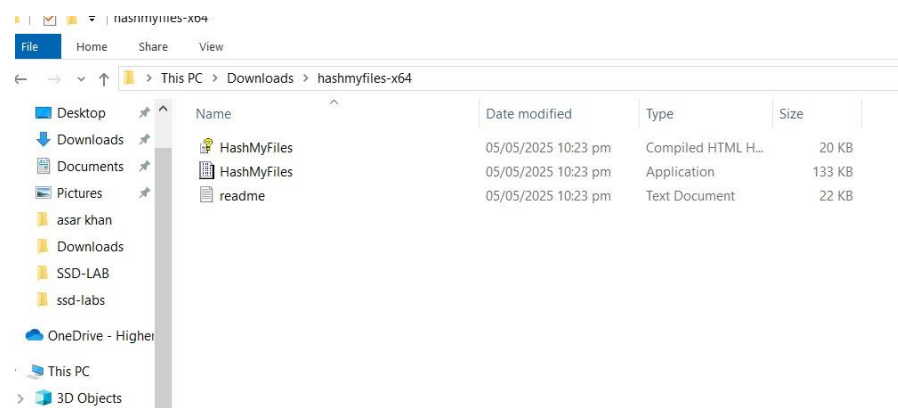
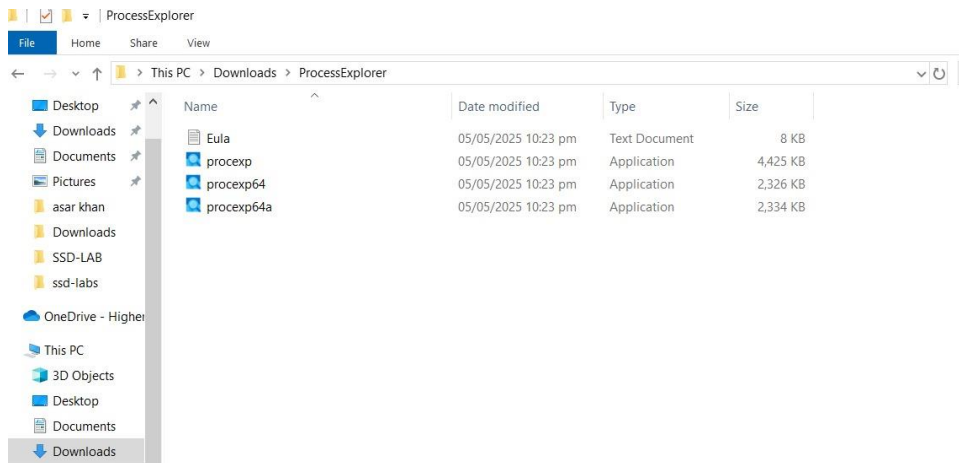
2. Tools Used:

- Process Explorer (Microsoft Sysinternals)
- Process Monitor (Microsoft Sysinternals)
- PEStudio (Winitor)
- Wireshark (Network Protocol Analyzer)
- HashMyFiles (NirSoft)

3. Step 1: Setup Environment

- A separate Windows PC was used with no internet connection.
- Installed all analysis tools listed above.





4. Step 2: Getting the Malware Sample

- A test malware sample was downloaded from a safe repository.
- Stored safely in a folder named "MalwareSamples."

> This PC > Local Disk (C:) > MalwareSamples >

| Name | Date modified | Type | Size |
|---------------------------------------|---------------------|-------------|------|
| 4a4cbb675bc99e47d5aa97b87581cc4eea... | 05/05/2025 11:00 pm | File folder | |
| 2812aa65f601ae9465881779d1603bd2b4... | 05/05/2025 10:59 pm | File folder | |

5. Step 3: Static Analysis

- Hashes were calculated using HashMyFiles.
 - MD5: 13db9e0f18443b2d6059c334d32a5cc7
 - SHA1: 7f40eae29cc7b26538705a78c29dd311bed54253
 - SHA256:
2812aa65f601ae9465881779d1603bd2b42ef073f36dcca9824ed1058881c5d6

| Filename | MD5 | SHA1 | CRC32 | SHA-256 |
|------------------------|----------------------------------|--|----------|---|
| 2812aa65f601ae94658... | 13db9e0f18443b2d6059c334d32a5cc7 | 7f40eae29cc7b26538705a78c29dd311bed54... | da6ea8ce | 2812aa65f601ae9465881779d1603bd2b42ef0... |

| | |
|-----------|--|
| Filename: | 2812aa65f601ae9465881779d1603bd2b42ef073f36dcca9824ed1058881c5d6.exe |
| MD5: | 13db9e0f18443b2d6059c334d32a5cc7 |
| SHA1: | 7f40eae29cc7b26538705a78c29dd311bed54253 |
| CRC32: | da6ea8ce |
| SHA-256: | 2812aa65f601ae9465881779d1603bd2b42ef073f36dcca9824ed1058881c5d6 |

- VirusTotal lookup result:
 - Detection rate:56/72

56 / 72

Community Score

56/72 security vendors flagged this file as malicious

Reanalyze

Similar

More

2812aa65f601ae9465881779d1603bd2b42ef073f36dcca9824ed1058881c5d6

Size

45.00 KB

Last Analysis Date

3 hours ago

Stub.exe

peexe

assembly

long-sleeps

calls-wmi

detect-debug-environment

obfuscated

spreader

malware

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 7

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

trojan.asyncrat/msil

Threat categories

trojan dropper

Family labels

asyncrat msil marte

Security vendors' analysis

Do you want to automate checks?

| | | | |
|------------------|-----------------------------------|-------------|-----------------------------------|
| AhnLab-V3 | Trojan/Win32_RL_Generic.R358277 | Allbaba | Backdoor.MSIL/AsyncRat.511c4ff |
| AllCloud | Rat-Win/AsyncRAT.Stub | ALYac | Generic.AsyncRAT.Marte.B.FC9FB4DD |
| Arcabit | Generic.AsyncRAT.Marte.B.FC9FB4DD | Arctic Wolf | Unsafe |
| Avast | Win32:MalwareX-gen [Drp] | AVG | Win32:MalwareX-gen [Drp] |
| Avira (no cloud) | TR/Dropper.Gen | BitDefender | Generic.AsyncRAT.Marte.B.FC9FB4DD |

- PEStudio Analysis:

pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\malwaresamples\2812aa65f601ae9465881779d1603bd2b42ef073f36dcca9824ed1058881c5d6\2812aa65f601ae9465881779d1603bd2b42ef073f36dcca9824ed1058881c5d6.exe

file settings about

resamples\2812aa65f601ae9465881779d1603bd2b42ef073f36dcca9824ed1058881c5d6

rtors (virustotal > score)

rints (type > sha256)

otal (score > 56/72)

header (size > 64 bytes)

tub (size > 64 bytes)

header (n/a)

header (executable > 32-bit)

nal-header (subsystem > GUI)

ories (count > 5)

ins (count > 3)

es (count > 4)

its (flag > 11)

ts (n/a)

b-local-storage (n/a)

(module > name > AsyncClient.exe)

races (count > 2)

s (count > 1339)

p (n/a)

test (level > asinvoker)

n (OriginalFilename > Stub.exe)

kate (n/a)

by (n/a)

property

value

file

file > sha256

2812AA65F601AE9465881779D1603BD2B42EF073F36DCCA9824ED1058881C5D6

file > first 32 bytes (hex)

4D 5A 90 00 03 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

file > first 32 bytes (text)

MZ.....@.....

file > info

size: 46080 bytes, entropy: 5.454

file > type

executable, 32-bit, GUI

file > version

1.0.0.0

file > description

n/a

entry-point > first 32 bytes (hex)

FF 25 00 20 40 00

entry-point > location

0x0000C77E

file > signature

Microsoft Linker 8.0 | Microsoft Visual C# / Basic .NET | Microsoft.NET

stamps

stamp > compiler

Sun May 10 05:24:51 2020 (UTC)

stamp > debug

n/a

stamp > resource

n/a

stamp > import

n/a

stamp > export

n/a

names

file > name

c:\malwaresamples\2812aa65f601ae9465881779d1603bd2b42ef073f36dcca9824ed1058881c5d6\2812aa65f601ae9465881779d1603bd2b42ef073f36dcca9824ed1058881c5d6.exe

debug > file

n/a

export

n/a

version > original-file-name

Stub.exe

manifest

n/a

.NET > module > name

AsyncClient.exe

certificate > program-name

n/a

6. Step 4: Dynamic Analysis

- Process Explorer observed new processes created by the malware.
- Before execution:

File Options View Process Find Users Help

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|---------------------------|---------|---------------|-------------|-------|---------------------------------|-----------------------|
| Registry | | 6,188 K | 94,212 K | 100 | | |
| System Idle Process | | 60 K | 8 K | 0 | | |
| System | 1.84 | 196 K | 112 K | 4 | | |
| Interrupts | 2.21 | 0 K | 0 K | n/a | Hardware Interrupts and DPCs | |
| smss.exe | | 1,072 K | 1,044 K | 364 | | |
| Memory Compression | < 0.01 | 1,332 K | 588,780 K | 2952 | | |
| csrss.exe | < 0.01 | 2,244 K | 6,444 K | 568 | | |
| wininit.exe | | 1,672 K | 7,044 K | 736 | | |
| services.exe | < 0.01 | 8,348 K | 11,196 K | 808 | | |
| svchost.exe | < 0.01 | 26,536 K | 42,736 K | 400 | Host Process for Windows S... | Microsoft Corporation |
| Path: | | 3,992 K | 11,700 K | 6720 | | |
| [Error opening process] | | 13,052 K | 15,568 K | 7244 | | |
| WmiPrvSE.exe | | 18,776 K | 26,980 K | 18408 | | |
| unsecapp.exe | | 1,404 K | 7,860 K | 10904 | | |
| StartMenuExperienceHo... | | 32,904 K | 89,508 K | 5756 | | |
| RuntimeBroker.exe | | 7,960 K | 33,048 K | 15008 | Runtime Broker | Microsoft Corporation |
| SearchApp.exe | Susp... | 227,964 K | 326,460 K | 10372 | Search application | Microsoft Corporation |
| RuntimeBroker.exe | | 15,492 K | 48,516 K | 15976 | Runtime Broker | Microsoft Corporation |
| ShellExperienceHost.exe | Susp... | 74,012 K | 124,820 K | 6244 | Windows Shell Experience H... | Microsoft Corporation |
| RuntimeBroker.exe | | 10,348 K | 37,876 K | 9808 | Runtime Broker | Microsoft Corporation |
| LockApp.exe | Susp... | 23,364 K | 65,244 K | 12164 | LockApp.exe | Microsoft Corporation |
| RuntimeBroker.exe | | 9,384 K | 29,252 K | 14204 | Runtime Broker | Microsoft Corporation |
| RuntimeBroker.exe | | 12,136 K | 42,628 K | 11868 | Runtime Broker | Microsoft Corporation |
| PhoneExperienceHoste... | < 0.01 | 54,124 K | 144,104 K | 7972 | Microsoft Phone Link | Microsoft Corporation |
| RuntimeBroker.exe | | 2,924 K | 15,808 K | 672 | Runtime Broker | Microsoft Corporation |
| ApplicationFrameHoste... | | 10,572 K | 35,248 K | 6508 | Application Frame Host | Microsoft Corporation |
| TextInputHost.exe | < 0.01 | 18,424 K | 63,112 K | 10504 | | Microsoft Corporation |
| dllhost.exe | | 5,564 K | 14,032 K | 3836 | COM Surrogate | Microsoft Corporation |
| dllhost.exe | | 1,936 K | 9,372 K | 7812 | COM Surrogate | Microsoft Corporation |
| CompPkgSrv.exe | | 1,700 K | 8,476 K | 12104 | Component Package Suppor... | Microsoft Corporation |
| RuntimeBroker.exe | | 2,752 K | 13,600 K | 1584 | Runtime Broker | Microsoft Corporation |
| FileCoAuth.exe | | 5,640 K | 23,036 K | 2592 | Microsoft OneDriveFile Co-A... | Microsoft Corporation |
| WmiPrvSE.exe | 3.68 | 13,148 K | 20,168 K | 4152 | | |
| unsecapp.exe | | 1,372 K | 7,704 K | 14736 | Sink to receive asynchronous... | Microsoft Corporation |
| SystemSettingsBroker.e... | | 7,572 K | 30,316 K | 14560 | System Settings Broker | Microsoft Corporation |
| SystemSettings.exe | Susp... | 28,500 K | 2,088 K | 15016 | Settings | Microsoft Corporation |
| UserOOBEBroker.exe | | 1,908 K | 9,408 K | 5968 | User OOBEBroker | Microsoft Corporation |
| smartscreen.exe | < 0.01 | 8,296 K | 23,800 K | 2652 | Windows Defender SmartScr... | Microsoft Corporation |
| ScreenClippingHost.exe | 2.94 | 12,760 K | 46,580 K | 12180 | | Microsoft Corporation |
| svchost.exe | 0.74 | 22,488 K | 24,696 K | 976 | Host Process for Windows S... | Microsoft Corporation |
| svchost.exe | | 3,512 K | 10,696 K | 1080 | Host Process for Windows S... | Microsoft Corporation |
| svchost.exe | | 2,852 K | 10,644 K | 1200 | Host Process for Windows S... | Microsoft Corporation |
| svchost.exe | | 2,936 K | 9,760 K | 1296 | Host Process for Windows S... | Microsoft Corporation |
| svchost.exe | < 0.01 | 18,000 K | 16,524 K | 1308 | Host Process for Windows S... | Microsoft Corporation |
| svchost.exe | | 2,548 K | 8,512 K | 1320 | Host Process for Windows S... | Microsoft Corporation |

- After execution:

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-PJ615MU\Aizaz]

File Options View Process Find Users Help

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|--------------------------------|--------|---------------|-------------|-------|-------------------------------------|------------------------------|
| AggregatorHost.exe | | 4,120 K | 9,092 K | 7728 | | |
| amdfendrsr.exe | | 3,788 K | 6,576 K | 2212 | AMD Crash Defender Service | Advanced Micro Devices, L... |
| atieclxx.exe | | 2,896 K | 13,956 K | 16140 | | |
| atiesrx.exe | | 1,532 K | 6,480 K | 2236 | AMD External Events Service... | AMD |
| audiodg.exe | | 6,488 K | 12,400 K | 10024 | | |
| browser_assistant.exe | | 5,420 K | 20,416 K | 9688 | Opera Browser Assistant | Opera Software |
| chrome.exe | < 0.01 | 181,376 K | 259,924 K | 9408 | Google Chrome | Google LLC |
| conhost.exe | | 6,224 K | 5,820 K | 6568 | | |
| conhost.exe | | 6,700 K | 13,612 K | 5480 | Console Window Host | Microsoft Corporation |
| csrss.exe | | 2,212 K | 6,484 K | 568 | | |
| csrss.exe | < 0.01 | 2,964 K | 6,956 K | 13720 | | |
| ctfmon.exe | | 22,000 K | 24,964 K | 16208 | | |
| CxMonSvc.exe | | 19,680 K | 20,628 K | 4436 | CxMonSvc | Conexant Systems, Inc |
| CxUtilSvc.exe | | 1,528 K | 7,552 K | 4456 | Utility Service | Conexant Systems, Inc. |
| dasHost.exe | | 3,516 K | 12,024 K | 16148 | | |
| dllhost.exe | | 4,056 K | 13,348 K | 2628 | COM Surrogate | Microsoft Corporation |
| dumpcap.exe | < 0.01 | 4,004 K | 8,728 K | 16240 | Dumpcap | The Wireshark developer ... |
| dwm.exe | < 0.01 | 163,328 K | 162,636 K | 3168 | | |
| explorer.exe | < 0.01 | 120,748 K | 205,244 K | 14128 | Windows Explorer | Microsoft Corporation |
| fontdrvhost.exe | | 2,264 K | 4,808 K | 592 | | |
| fontdrvhost.exe | | 4,500 K | 8,488 K | 11952 | | |
| fpCSEvtSvc.exe | | 7,092 K | 7,052 K | 4480 | | |
| HotKeyServiceUWP.exe | | 3,968 K | 15,620 K | 9812 | HP Hotkey UWP Service | HP Inc. |
| HPAudioAnalytics.exe | | 2,872 K | 13,332 K | 20328 | HP Hotkey UWP Service | HP Inc. |
| HPHotkeyNotification.exe | < 0.01 | 24,360 K | 31,852 K | 5920 | | |
| ibtsiva.exe | | 1,172 K | 5,184 K | 4512 | Intel(R) Wireless Bluetooth(R)... | Intel Corporation |
| IntelCpHDCPSvc.exe | | 1,376 K | 7,156 K | 1452 | Intel HD Graphics Drivers for ... | Intel Corporation |
| IntelCpHeciSvc.exe | | 1,408 K | 7,204 K | 1708 | IntelCpHeciSvc Executable | Intel Corporation |
| Interrupts | < 0.01 | 0 K | 0 K | n/a | Hardware Interrupts and DPCs | |
| LanWlanWwanSwitchingService... | | 3,696 K | 13,592 K | 4608 | HP LAN/WLAN/WWAN Switc... | HP Inc. |
| lsass.exe | < 0.01 | 12,296 K | 27,728 K | 816 | Local Security Authority Proc... | Microsoft Corporation |
| Memory Compression | | 1,568 K | 614,364 K | 2952 | | |
| Microsoft.SharePoint.exe | | 33,428 K | 11,180 K | 15560 | Microsoft SharePoint | Microsoft Corporation |
| MicTray64.exe | | 2,372 K | 7,784 K | 11708 | | |
| MpDefenderCoreService.exe | | 11,268 K | 19,500 K | 4668 | Antimalware Core Service | Microsoft Corporation |
| msdtc.exe | | 2,876 K | 9,092 K | 9660 | Microsoft Distributed Transac... | Microsoft Corporation |
| msedge.exe | | 43,220 K | 100,704 K | 8220 | Microsoft Edge | Microsoft Corporation |
| msedgewebview2.exe | | 42,480 K | 68,312 K | 18340 | Microsoft Edge WebView2 | Microsoft Corporation |
| MsMpEng.exe | | 303,480 K | 202,316 K | 4888 | Antimalware Service Executa... | Microsoft Corporation |
| MusNotiflycon.exe | | 3,284 K | 3,024 K | 5900 | MusNotiflycon.exe | Microsoft Corporation |
| OfficeClickToRun.exe | | 50,108 K | 47,148 K | 18228 | Microsoft Office Click-to-Run (...) | Microsoft Corporation |
| olk.exe | | 12,308 K | 10,316 K | 8252 | Microsoft Outlook | Microsoft Corporation |
| pestudio.exe | 25.17 | 1,767,896 K | 1,699,288 K | 14500 | Malware Initial Assessment ... | www.winitor.com |

Wireshark captured the following suspicious network traffic:

- IPs contacted: 150.171.22.12
- Domains contacted: akami cdn
-
- IPs contacted: 119.152.63.0/24
- Domains contacted: tencent cloud
-

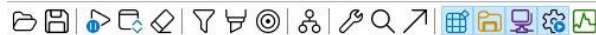
| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|----------------|----------------|----------|--------|--|
| 1089 | 115.575663 | 3.77.139.2 | 192.168.1.105 | TCP | 66 | [TCP Keep-Alive ACK] 443 → 51231 [ACK] Seq=1 Ack=2 Win=214 Len=0 SLE=1 SRE=2 |
| 1090 | 115.736714 | 192.168.1.105 | 172.217.19.234 | UDP | 71 | 59899 → 443 Len=29 |
| 1091 | 115.830457 | 192.168.1.105 | 172.217.19.234 | UDP | 71 | 59899 → 443 Len=29 |
| 1092 | 115.901274 | 172.217.19.234 | 192.168.1.105 | UDP | 70 | 443 → 59899 Len=28 |
| 1093 | 116.039161 | 204.79.197.222 | 192.168.1.105 | TCP | 54 | 443 → 51331 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 1094 | 117.299368 | 192.168.1.105 | 192.168.1.1 | DNS | 83 | Standard query 0x6fd7 A umarmira055.duckdns.org |
| 1095 | 117.301292 | 192.168.1.105 | 157.240.227.61 | TCP | 54 | 51362 → 5222 [FIN, ACK] Seq=813 Ack=2018 Win=131584 Len=0 |
| 1096 | 117.540319 | 192.168.1.1 | 192.168.1.105 | DNS | 99 | Standard query response 0x6fd7 A umarmira055.duckdns.org A 192.169.69.26 |
| 1097 | 117.540708 | 192.168.1.105 | 192.169.69.26 | TCP | 66 | 51367 → 7031 [SYN] Seq=0 Win=51200 Len=0 MSS=1460 WS=1 SACK_PERM |
| 1098 | 117.511188 | 192.168.1.105 | 157.240.227.61 | TCP | 54 | [TCP Retransmission] 51362 → 5222 [FIN, ACK] Seq=813 Ack=2018 Win=131584 Len=0 |
| 1099 | 117.657738 | 157.240.227.61 | 192.168.1.105 | TCP | 66 | 5222 → 51362 [ACK] Seq=2018 Ack=814 Win=67840 Len=0 SLE=813 SRE=814 |
| 1100 | 117.739451 | 157.240.227.61 | 192.168.1.105 | TCP | 54 | 5222 → 51362 [FIN, ACK] Seq=2018 Ack=814 Win=67840 Len=0 |
| 1101 | 117.739493 | 192.168.1.105 | 157.240.227.61 | TCP | 54 | 51362 → 5222 [ACK] Seq=814 Ack=2019 Win=131584 Len=0 |
| 1102 | 118.004878 | 192.169.69.26 | 192.168.1.105 | TCP | 58 | 7031 → 51367 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 |
| 1103 | 118.004933 | 192.168.1.105 | 192.169.69.26 | TCP | 54 | 51367 → 7031 [ACK] Seq=1 Ack=1 Win=51200 Len=0 |
| 1104 | 118.005261 | 192.168.1.105 | 192.169.69.26 | TLSv1 | 149 | Client Hello |
| 1105 | 118.008705 | 192.169.69.26 | 192.168.1.105 | TCP | 54 | 7031 → 51367 [RST] Seq=1 Win=0 Len=0 |
| 1106 | 118.011731 | 40.99.60.2 | 192.168.1.105 | TLSv1.2 | 95 | Application Data |

> Frame 1: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{39308297-56-0000-14-c0-26-8f-c0-f8-63-3f-cc-0a-fb-08-00-45-00} ... f...c ?...-E-
 > Ethernet II, Src: Intelces:0a:fb:(f8:63:3f:cc:0a:fb), Dst: TnlkTechno:66:8f:c0:(14:ce:20:66:8f:c0) 0018 00 3f e6 fc 40 00 80 11 a4 e0 c0 a8 01 69 96 ab ...?..@... ..i..

Process Monitor recorded these changes:

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help



| Time o... | Process Name | PID | Operation | Path | Result | Detail |
|-------------|------------------|------|------------|--|----------------|----------------------|
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows | SUCCESS | Desired Access: E... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\System32\wow64log.dll | NAME NOT FOUND | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\MalwareSamples\2812aa65f601ae94... | SUCCESS | Desired Access: E... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\mscoree.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\mscoree.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\apphelp.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\apphelp.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\MalwareSamples\2812aa65f601ae94... | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\ntdll.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\mscoree.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\kernel32.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\KernelBase.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\apppatch\sysmain.sdb | SUCCESS | Desired Access: G... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\MalwareSamples\2812aa65f601ae94... | SUCCESS | Desired Access: G... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\apppatch\sysmain.sdb | SUCCESS | Desired Access: G... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\MalwareSamples\2812aa65f601ae94... | SUCCESS | Desired Access: G... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\msvcr7.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\rpcrt4.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\bcrypt.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\sechost.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\advapi32.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\MSCOREE.DL... | NAME NOT FOUND | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\Microsoft.NET\Framework\... | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\Microsoft.NET\Framework\... | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\Microsoft.NET\Framework\... | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\MSCOREE.DL... | NAME NOT FOUND | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\Microsoft.NET\Framework\... | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\Microsoft.NET\Framework\... | NAME NOT FOUND | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\Microsoft.NET\Framework\... | NAME NOT FOUND | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\Microsoft.NET\Framework\... | NAME NOT FOUND | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\Microsoft.NET\Framework\... | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\shlwapi.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\MalwareSamples\2812aa65f601ae94... | NAME NOT FOUND | Desired Access: G... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\MalwareSamples\2812aa65f601ae94... | SUCCESS | Desired Access: G... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\MalwareSamples\2812aa65f601ae94... | SUCCESS | Desired Access: G... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\kernel.appcor... | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\kernel.appcor... | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\kernel.appcor... | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\version.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\version.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\SysWOW64\version.dll | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\Microsoft.NET\Framework\... | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\Microsoft.NET\Framework\... | SUCCESS | Desired Access: G... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\Microsoft.NET\Framework\... | SUCCESS | Desired Access: R... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\Microsoft.NET\Framework\... | SUCCESS | Desired Access: G... |
| 1:11:41.... | 2812aa65f601a... | 5432 | CreateFile | C:\Windows\Microsoft.NET\Framework\... | SUCCESS | Desired Access: R... |

0.034% Backed by virtual memory

7. Step 5: Findings

- New processes created:
 - C:\Users\Ahmad\AppData\Local\Temp\evilspawn.exe
 - C:\Windows\System32\cmd.exe
- Files/Registry modified: - C:\Users\Ahmad\AppData\Local\Temp\
 - C:\Windows\System32\
- Network traffic to suspicious IPs/domains: 150.171.22.12/ akami cdn
 - 119.152.63.0/24/tencent cloud

8. Conclusion:

This malware sample exhibited behaviors such as process injection, file modification, and network beaconing. Static and dynamic analysis provided insight into its techniques and indicators of compromise. The analysis environment was kept isolated to ensure safety during testing.