Sample 1

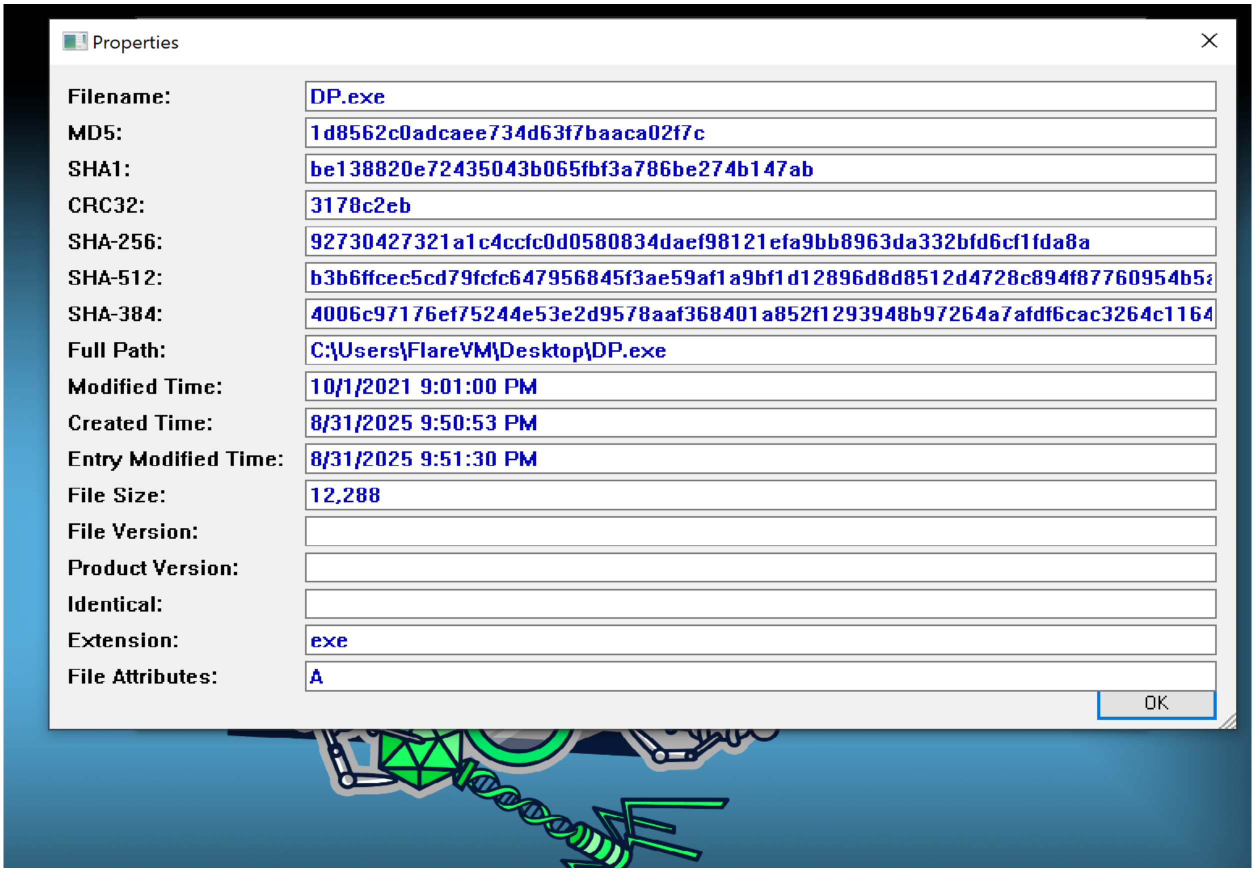
Ujjwal Kumar

Reg no:- 12220072

Roll no: 61

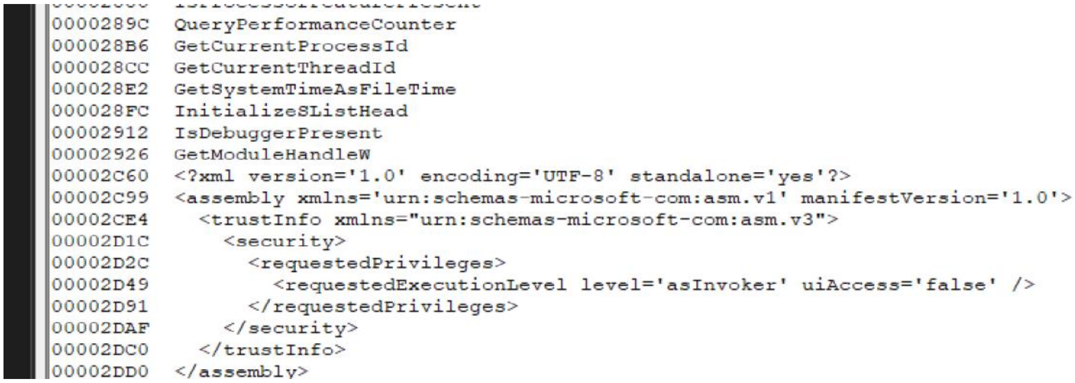
Static Analysis

HashMyFiles – Generates MD5/SHA256 hash of the malware to uniquely identify it.

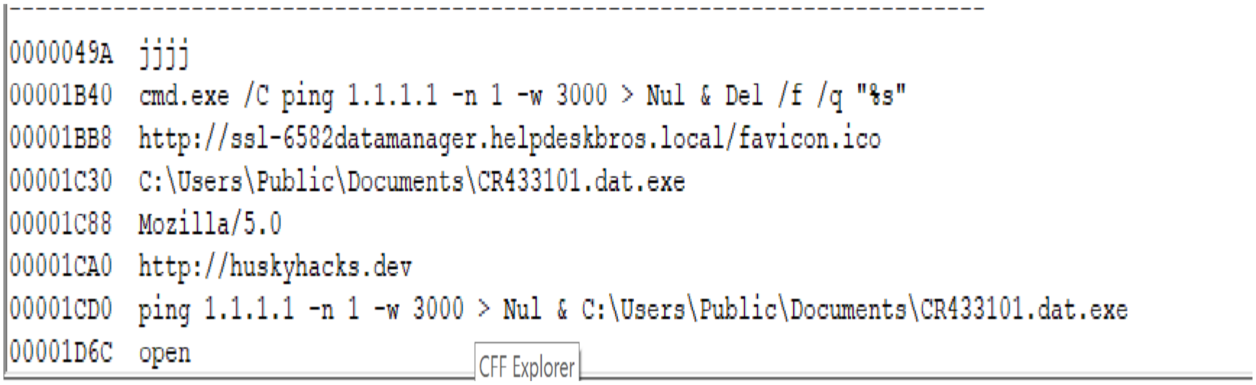


Filename:	DP.exe
MD5:	1d8562c0adcaee734d63f7baaca02f7c
SHA1:	be138820e72435043b065fbf3a786be274b147ab
CRC32:	3178c2eb
SHA-256:	92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a
SHA-512:	b3b6ffcec5cd79fcfc647956845f3ae59af1a9bf1d12896d8d8512d4728c894f87760954b5
SHA-384:	4006c97176ef75244e53e2d9578aaf368401a852f1293948b97264a7afdf6cac3264c1164
Full Path:	C:\Users\FlareVM\Desktop\DP.exe
Modified Time:	10/1/2021 9:01:00 PM
Created Time:	8/31/2025 9:50:53 PM
Entry Modified Time:	8/31/2025 9:51:30 PM
File Size:	12,288
File Version:	
Product Version:	
Identical:	
Extension:	exe
File Attributes:	A

Strings: Extracts human-readable strings from malware binaries.

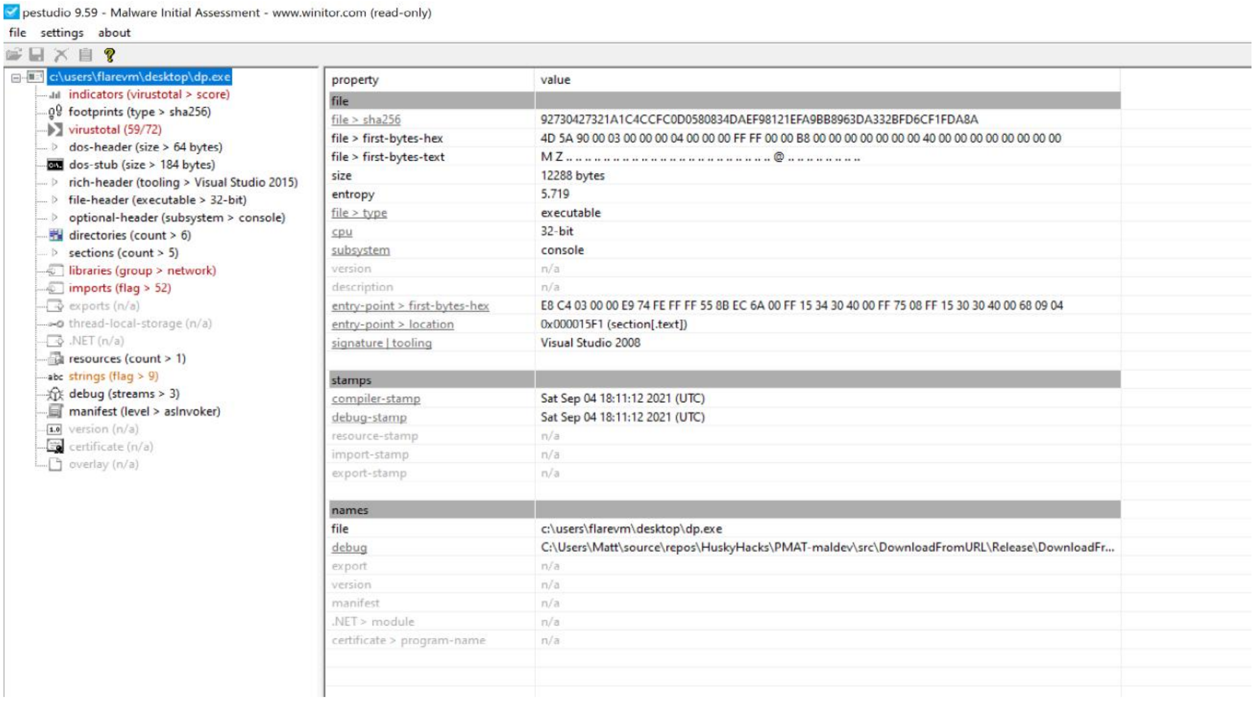


```
0000289C  QueryPerformanceCounter
000028B6  GetCurrentProcessId
000028CC  GetCurrentThreadId
000028E2  GetSystemTimeAsFileTime
000028FC  InitializeSListHead
00002912  IsDebuggerPresent
00002926  GetModuleHandleW
00002C60  <?xml version='1.0' encoding='UTF-8' standalone='yes'?>
00002C99  <assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
00002CE4    <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
00002D1C      <security>
00002D2C        <requestedPrivileges>
00002D49          <requestedExecutionLevel level='asInvoker' uiAccess='false' />
00002D91        </requestedPrivileges>
00002DAF      </security>
00002DC0    </trustInfo>
00002DD0  </assembly>
```



```
------------------------------------------------------------------------------
0000049A  jjjj
00001B40  cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
00001BB8  http://ssl-6582datamanager.helpdeskbros.local/favicon.ico
00001C30  C:\Users\Public\Documents\CR433101.dat.exe
00001C88  Mozilla/5.0
00001CA0  http://huskyhacks.dev
00001CD0  ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe
00001D6C  open
```

PEStudio – Analysis Portable Executable (PE) structure, entropy, imports/exports, suspicious indicators without executing the file

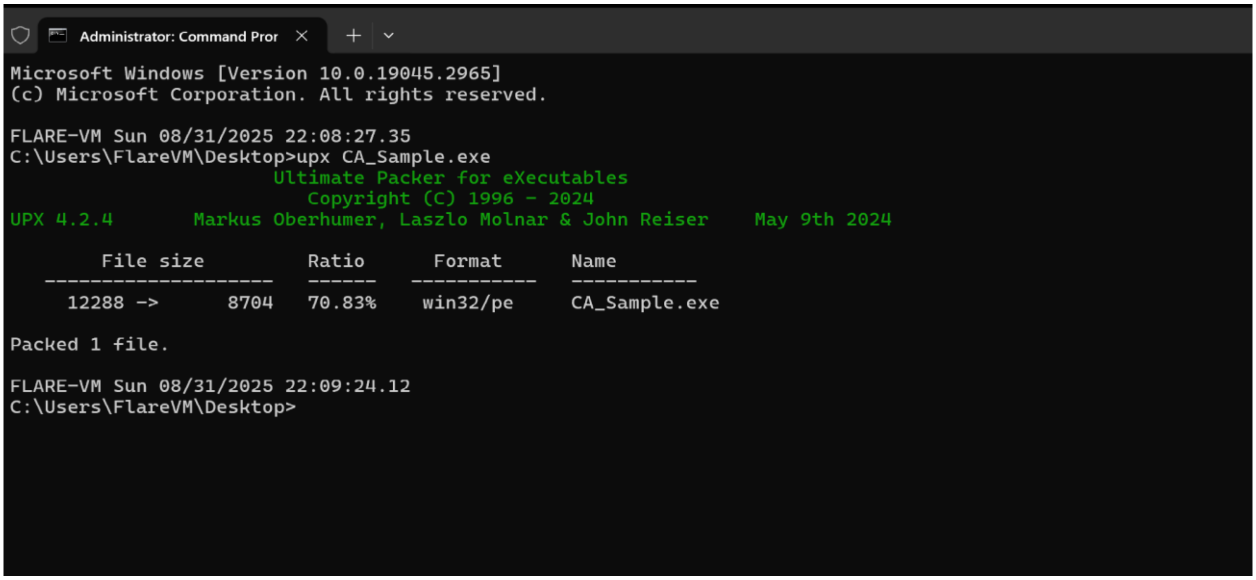


pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)

```
c:\users\flarevm\desktop\dp.exe
  indicators (virustotal > score)
  footprints (type > sha256)
  virustotal (59/72)
  dos-header (size > 64 bytes)
  dos-stub (size > 184 bytes)
  rich-header (tooling > Visual Studio 2015)
  file-header (executable > 32-bit)
  optional-header (subsystem > console)
  directories (count > 6)
  sections (count > 5)
  libraries (group > network)
  imports (flag > 52)
  exports (n/a)
  thread-local-storage (n/a)
  .NET (n/a)
  resources (count > 1)
  strings (flag > 9)
  debug (streams > 3)
  manifest (level > asInvoker)
  version (n/a)
  certificate (n/a)
  overlay (n/a)
```

property	value
file	
file > sha256	92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A
file > first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
file > first-bytes-text	M Z .. .. @ .. ..
size	12288 bytes
entropy	5.719
file > type	executable
cpu	32-bit
subsystem	console
version	n/a
description	n/a
entry-point > first-bytes-hex	E8 C4 03 00 00 E9 74 FE FF FF 55 8B EC 6A 00 FF 15 34 30 40 00 FF 75 08 FF 15 30 30 40 00 68 09 04
entry-point > location	0x000015F1 (section[.text])
signature | tooling	Visual Studio 2008
stamps	
compiler-stamp	Sat Sep 04 18:11:12 2021 (UTC)
debug-stamp	Sat Sep 04 18:11:12 2021 (UTC)
resource-stamp	n/a
import-stamp	n/a
export-stamp	n/a
names	
file	c:\users\flarevm\desktop\dp.exe
debug	C:\Users\Matt\source\repos\HuskyHacks\PMAT-maldev\src\DownloadFromURL\Release\DownloadFr...
export	n/a
version	n/a
manifest	n/a
.NET > module	n/a
certificate > program-name	n/a

Convert To Packed through UPX



Administrator: Command Pror

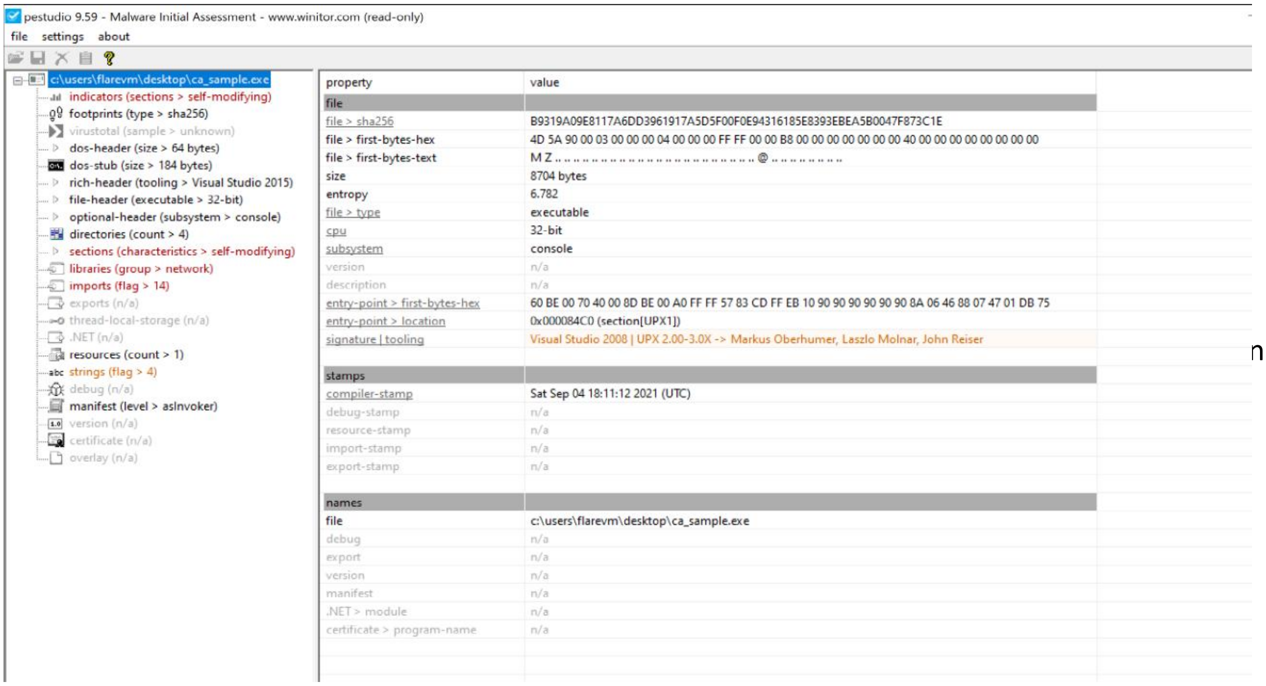
```
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

FLARE-VM Sun 08/31/2025 22:08:27.35
C:\Users\FlareVM\Desktop>upx CA_Sample.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2024
UPX 4.2.4       Markus Oberhumer, Laszlo Molnar & John Reiser    May 9th 2024

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     12288 ->      8704   70.83%    win32/pe     CA_Sample.exe

Packed 1 file.

FLARE-VM Sun 08/31/2025 22:09:24.12
C:\Users\FlareVM\Desktop>
```



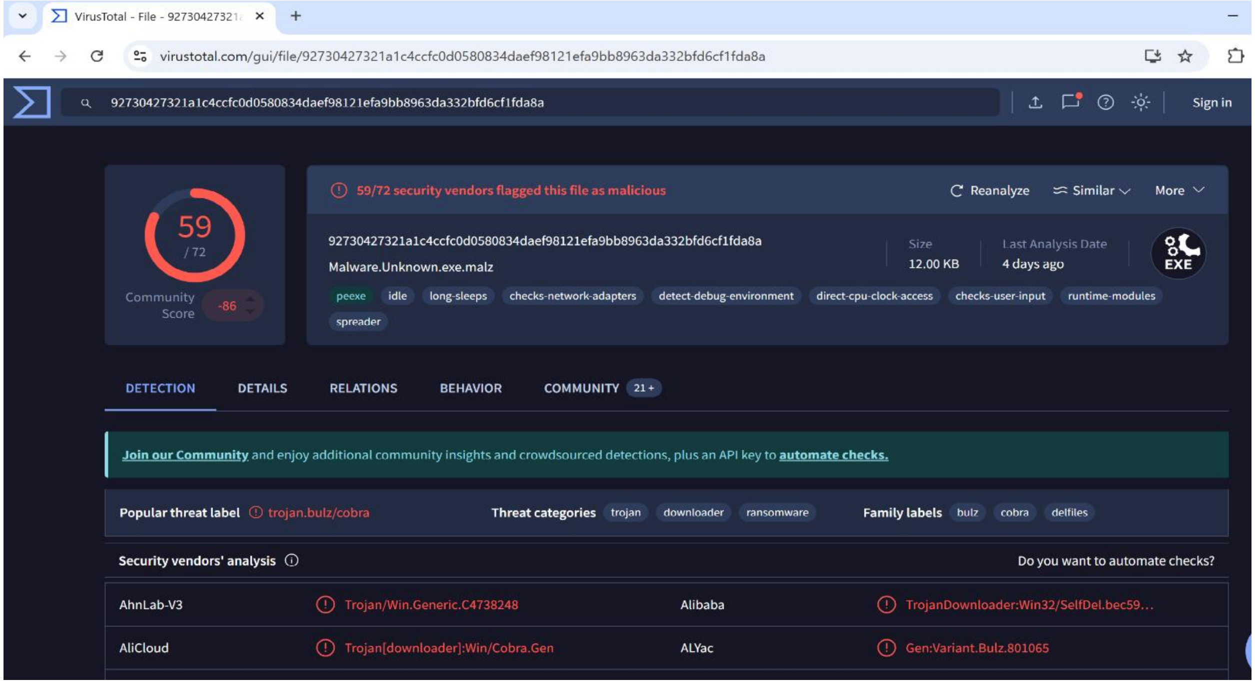
pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)

c:\users\flarevm\desktop\ca_sample.exe
- indicators (sections > self-modifying)
- footprints (type > sha256)
- virustotal (sample > unknown)
- dos-header (size > 64 bytes)
- dos-stub (size > 184 bytes)
- rich-header (tooling > Visual Studio 2015)
- file-header (executable > 32-bit)
- optional-header (subsystem > console)
- directories (count > 4)
- sections (characteristics > self-modifying)
- libraries (group > network)
- imports (flag > 14)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (count > 1)
- strings (flag > 4)
- debug (n/a)
- manifest (level > asInvoker)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

property	value
file	
file > sha256	B9319A09E8117A6DD3961917A5D5F00F0E94316185E8393EBEA5B0047F873C1E
file > first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
file > first-bytes-text	M Z .. .. @ .. ..
size	8704 bytes
entropy	6.782
file > type	executable
cpu	32-bit
subsystem	console
version	n/a
description	n/a
entry-point > first-bytes-hex	60 BE 00 70 40 00 8D BE 00 A0 FF FF 57 83 CD FF EB 10 90 90 90 90 90 90 8A 06 46 88 07 47 01 DB 75
entry-point > location	0x000084C0 (section[UPX1])
signature | tooling	Visual Studio 2008 | UPX 2.00-3.0X -> Markus Oberhumer, Laszlo Molnar, John Reiser
stamps	
compiler-stamp	Sat Sep 04 18:11:12 2021 (UTC)
debug-stamp	n/a
resource-stamp	n/a
import-stamp	n/a
export-stamp	n/a
names	
file	c:\users\flarevm\desktop\ca_sample.exe
debug	n/a
export	n/a
version	n/a
manifest	n/a
.NET > module	n/a
certificate > program-name	n/a

n

VirusTotal – Online multi-antivirus scanner to detect known malware and review AV detection results.



virustotal.com/gui/file/92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a

92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a

59 / 72

Community Score -86

59/72 security vendors flagged this file as malicious

92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a
Malware.Unknown.exe.malz

Size 12.00 KB

Last Analysis Date 4 days ago

peexe idle long-sleeps checks-network-adapters detect-debug-environment direct-cpu-clock-access checks-user-input runtime-modules spreader

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

Popular threat label trojan.bulz/cobra

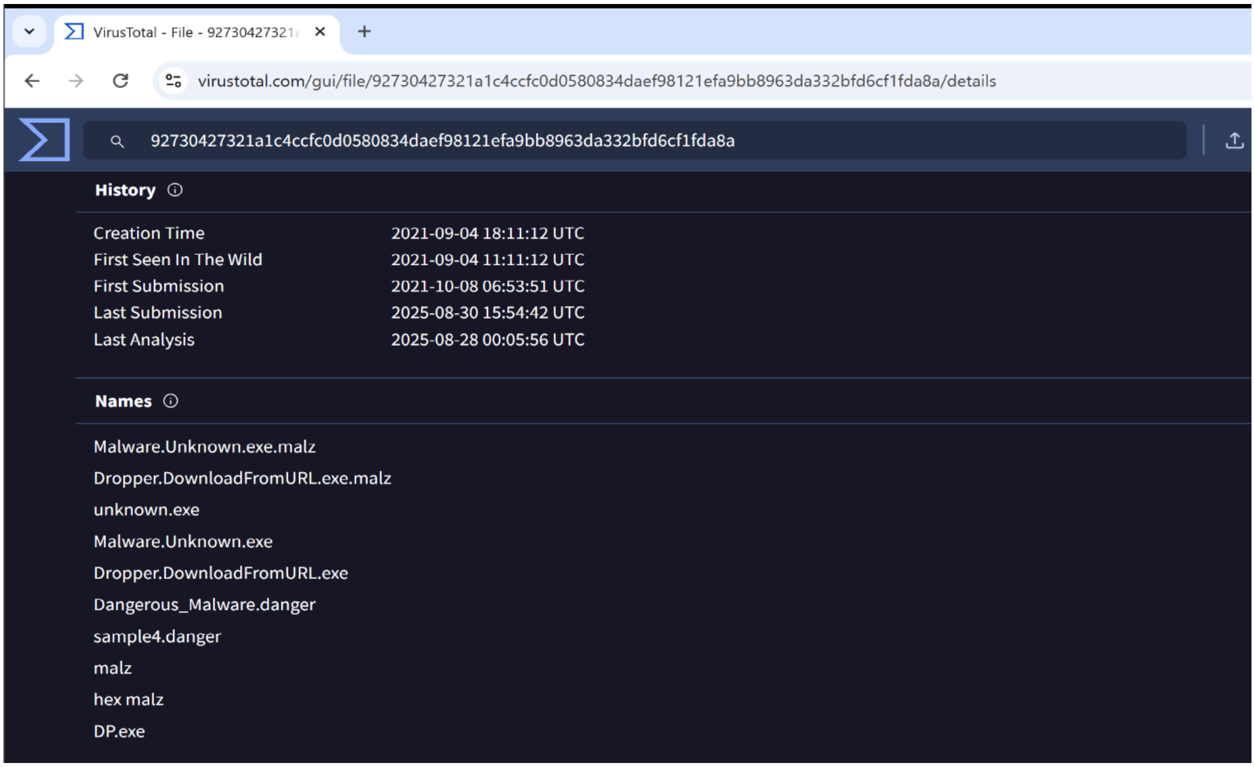
Threat categories trojan downloader ransomware

Family labels bulz cobra delfiles

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win.Generic.C4738248	Alibaba	TrojanDownloader:Win32/SelfDel.bec59...
AliCloud	Trojan[downloader]:Win/Cobra.Gen	ALYac	Gen:Variant.Bulz.801065



virustotal.com/gui/file/92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a/details

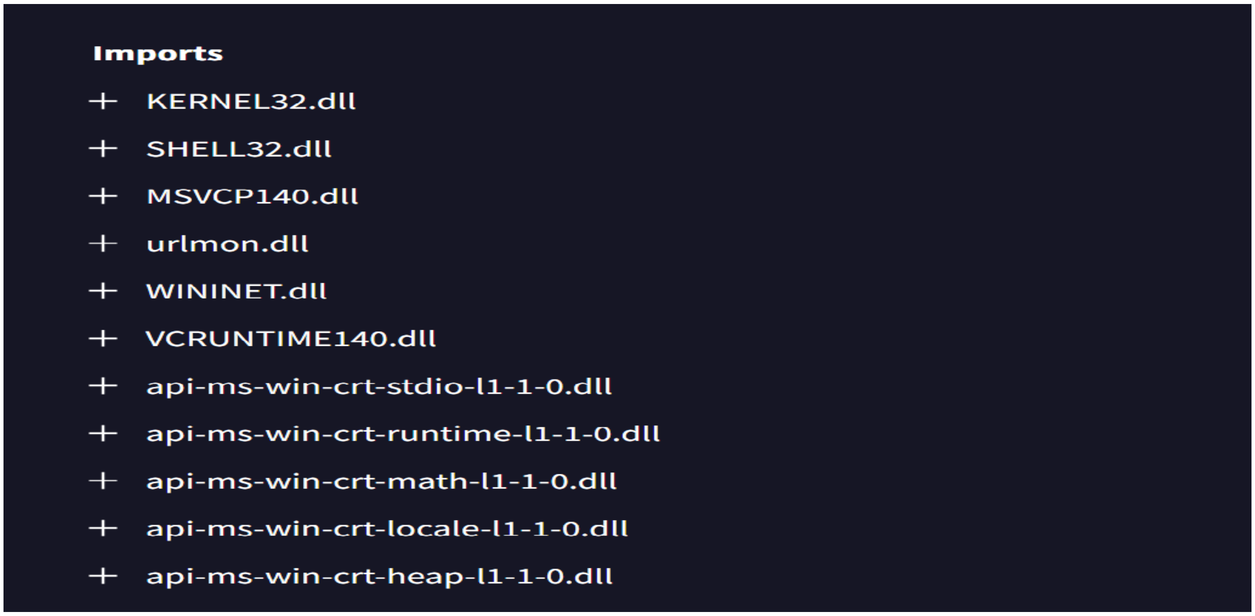
92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a

History

Creation Time	2021-09-04 18:11:12 UTC
First Seen In The Wild	2021-09-04 11:11:12 UTC
First Submission	2021-10-08 06:53:51 UTC
Last Submission	2025-08-30 15:54:42 UTC
Last Analysis	2025-08-28 00:05:56 UTC

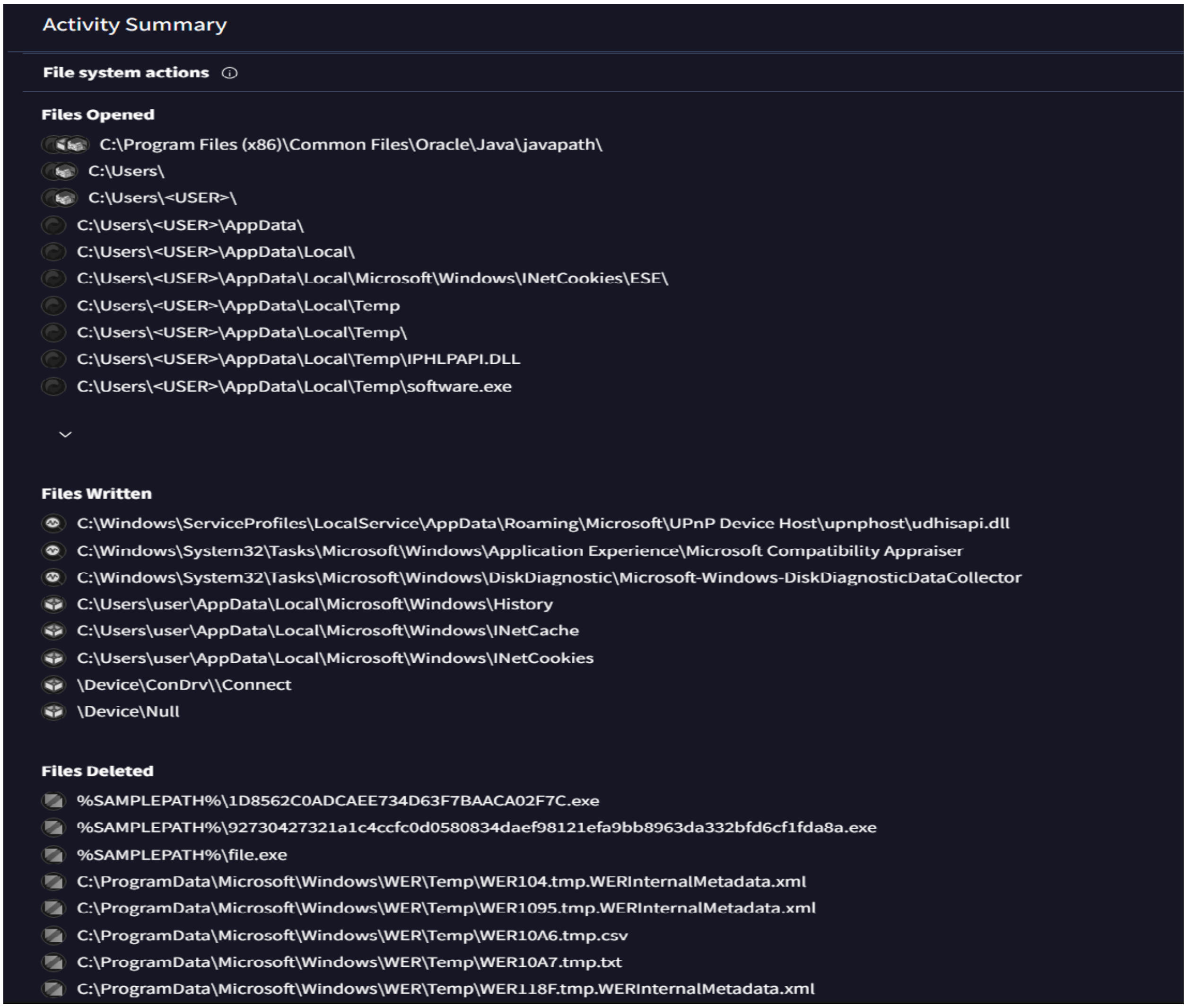
Names

Malware.Unknown.exe.malz
Dropper.DownloadFromURL.exe.malz
unknown.exe
Malware.Unknown.exe
Dropper.DownloadFromURL.exe
Dangerous_Malware.danger
sample4.danger
malz
hex malz
DP.exe



Imports

- + KERNEL32.dll
- + SHELL32.dll
- + MSVCP140.dll
- + urlmon.dll
- + WININET.dll
- + VCRUNTIME140.dll
- + api-ms-win-crt-stdio-l1-1-0.dll
- + api-ms-win-crt-runtime-l1-1-0.dll
- + api-ms-win-crt-math-l1-1-0.dll
- + api-ms-win-crt-locale-l1-1-0.dll
- + api-ms-win-crt-heap-l1-1-0.dll



Activity Summary

File system actions ⓘ

Files Opened

```
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\
C:\Users\
C:\Users\<USER>\
C:\Users\<USER>\AppData\
C:\Users\<USER>\AppData\Local\
C:\Users\<USER>\AppData\Local\Microsoft\Windows\INetCookies\ESE\
C:\Users\<USER>\AppData\Local\Temp
C:\Users\<USER>\AppData\Local\Temp\
C:\Users\<USER>\AppData\Local\Temp\IPHLPAPI.DLL
C:\Users\<USER>\AppData\Local\Temp\software.exe
```

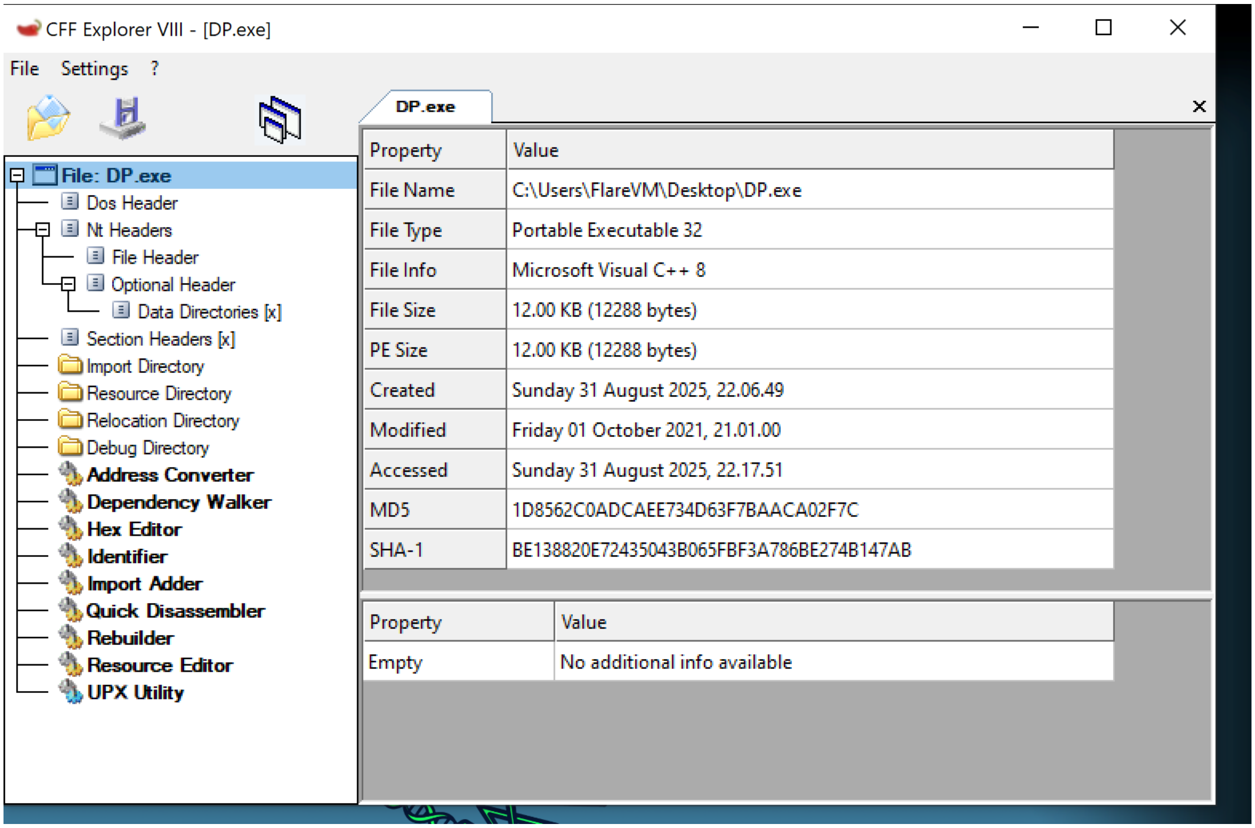
Files Written

```
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\UPnP Device Host\upnphost\udhisapi.dll
C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser
C:\Windows\System32\Tasks\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticDataCollector
C:\Users\user\AppData\Local\Microsoft\Windows\History
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies
\Device\ConDrv\\Connect
\Device\Null
```

Files Deleted

```
%SAMPLEPATH%\1D8562C0ADCAEE734D63F7BAACA02F7C.exe
%SAMPLEPATH%\92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a.exe
%SAMPLEPATH%\file.exe
C:\ProgramData\Microsoft\Windows\WER\Temp\WER104.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1095.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10A6.tmp.csv
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10A7.tmp.txt
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118F.tmp.WERInternalMetadata.xml
```

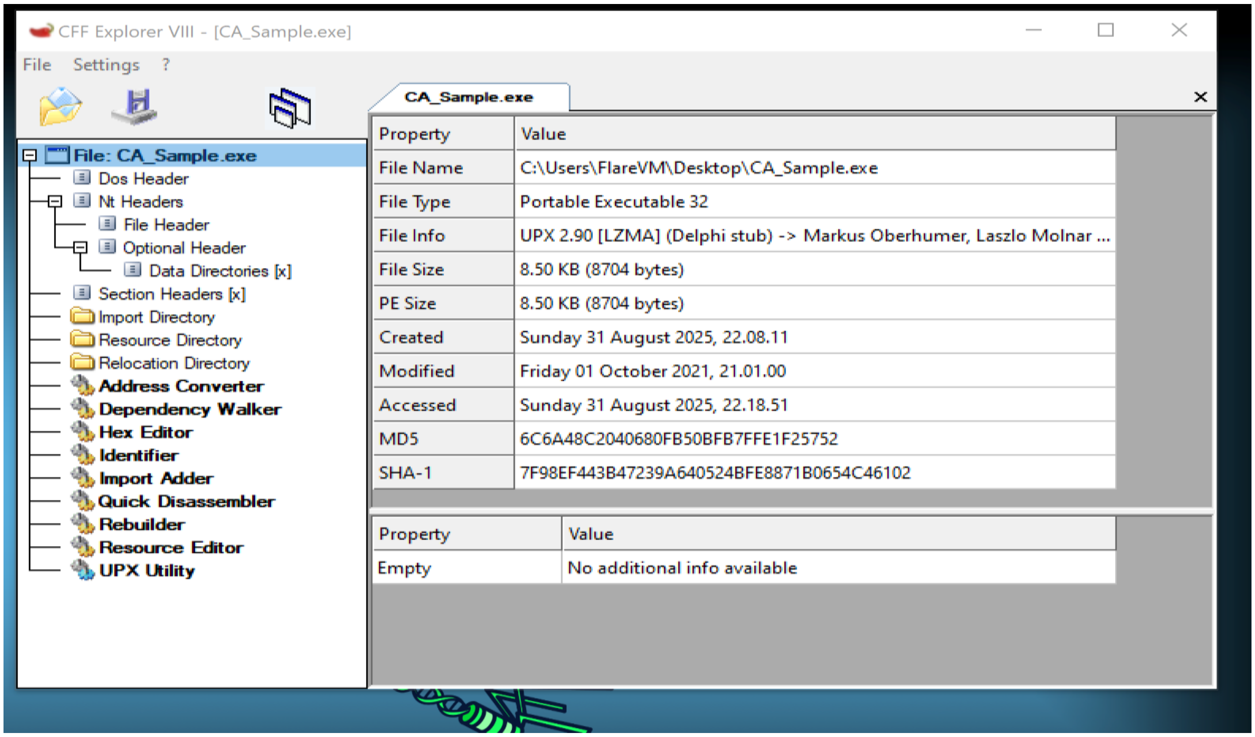
CFF Explorer for unpacked: CFF Explorer was used to compare unpacked vs. packed binaries for anomalies.



Property	Value
File Name	C:\Users\FlareVM\Desktop\DP.exe
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 8
File Size	12.00 KB (12288 bytes)
PE Size	12.00 KB (12288 bytes)
Created	Sunday 31 August 2025, 22.06.49
Modified	Friday 01 October 2021, 21.01.00
Accessed	Sunday 31 August 2025, 22.17.51
MD5	1D8562C0ADCAEE734D63F7BAACA02F7C
SHA-1	BE138820E72435043B065FBF3A786BE274B147AB

Property	Value
Empty	No additional info available

CFF explorer for packed:

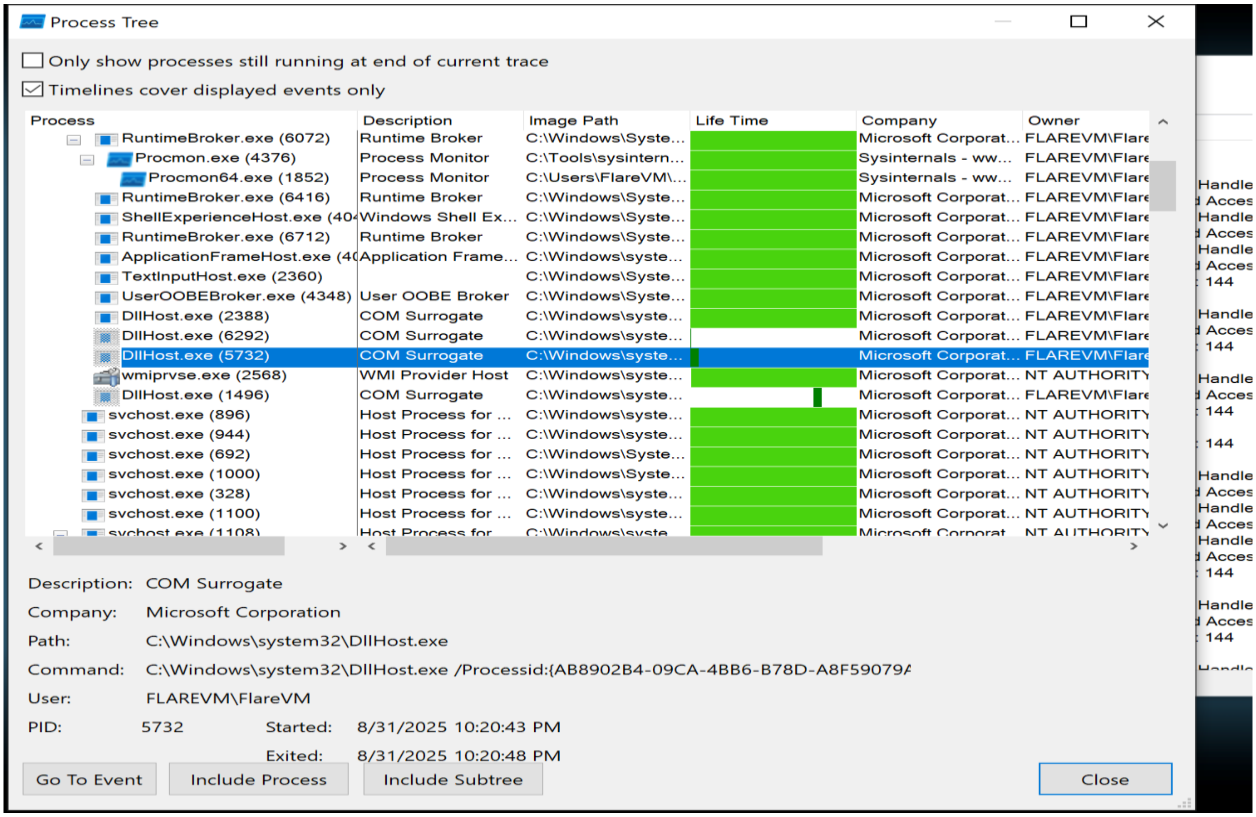


Property	Value
File Name	C:\Users\FlareVM\Desktop\CA_Sample.exe
File Type	Portable Executable 32
File Info	UPX 2.90 [LZMA] (Delphi stub) -> Markus Oberhumer, Laszlo Molnar ...
File Size	8.50 KB (8704 bytes)
PE Size	8.50 KB (8704 bytes)
Created	Sunday 31 August 2025, 22.08.11
Modified	Friday 01 October 2021, 21.01.00
Accessed	Sunday 31 August 2025, 22.18.51
MD5	6C6A48C2040680FB50BFB7FFE1F25752
SHA-1	7F98EF443B47239A640524BFE8871B0654C46102

Property	Value
Empty	No additional info available

DYNAMIC ANALYSIS

ProcMon (Process Monitor) – Monitors real-time system activity (file, registry, network, process changes) during malware execution.



□ Only show processes still running at end of current trace

☑ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner
RuntimeBroker.exe (6072)	Runtime Broker	C:\Windows\Syste...	🟩	Microsoft Corporat...	FLAREVM\Flare
Procmon.exe (4376)	Process Monitor	C:\Tools\sysintern...	🟩	Sysinternals - ww...	FLAREVM\Flare
Procmon64.exe (1852)	Process Monitor	C:\Users\FlareVM\...	🟩	Sysinternals - ww...	FLAREVM\Flare
RuntimeBroker.exe (6416)	Runtime Broker	C:\Windows\Syste...	🟩	Microsoft Corporat...	FLAREVM\Flare
ShellExperienceHost.exe (40	Windows Shell Ex...	C:\Windows\Syste...	🟩	Microsoft Corporat...	FLAREVM\Flare
RuntimeBroker.exe (6712)	Runtime Broker	C:\Windows\Syste...	🟩	Microsoft Corporat...	FLAREVM\Flare
ApplicationFrameHost.exe (4	Application Frame...	C:\Windows\syste...	🟩	Microsoft Corporat...	FLAREVM\Flare
TextInputHost.exe (2360)		C:\Windows\Syste...	🟩	Microsoft Corporat...	FLAREVM\Flare
UserOOBEBroker.exe (4348)	User OOBE Broker	C:\Windows\Syste...	🟩	Microsoft Corporat...	FLAREVM\Flare
DllHost.exe (2388)	COM Surrogate	C:\Windows\syste...	🟩	Microsoft Corporat...	FLAREVM\Flare
DllHost.exe (6292)	COM Surrogate	C:\Windows\syste...		Microsoft Corporat...	FLAREVM\Flare
DllHost.exe (5732)	COM Surrogate	C:\Windows\syste...	▌	Microsoft Corporat...	FLAREVM\Flare
wmiprvse.exe (2568)	WMI Provider Host	C:\Windows\syste...	🟩	Microsoft Corporat...	NT AUTHORITY
DllHost.exe (1496)	COM Surrogate	C:\Windows\syste...	▌	Microsoft Corporat...	FLAREVM\Flare
svchost.exe (896)	Host Process for ...	C:\Windows\syste...	🟩	Microsoft Corporat...	NT AUTHORITY
svchost.exe (944)	Host Process for ...	C:\Windows\syste...	🟩	Microsoft Corporat...	NT AUTHORITY
svchost.exe (692)	Host Process for ...	C:\Windows\Syste...	🟩	Microsoft Corporat...	NT AUTHORITY
svchost.exe (1000)	Host Process for ...	C:\Windows\Syste...	🟩	Microsoft Corporat...	NT AUTHORITY
svchost.exe (328)	Host Process for ...	C:\Windows\syste...	🟩	Microsoft Corporat...	NT AUTHORITY
svchost.exe (1100)	Host Process for ...	C:\Windows\syste...	🟩	Microsoft Corporat...	NT AUTHORITY
svchost.exe (1108)	Host Process for	C:\Windows\syste	🟩	Microsoft Corporat	NT AUTHORITY

Description: COM Surrogate

Company: Microsoft Corporation

Path: C:\Windows\system32\DllHost.exe

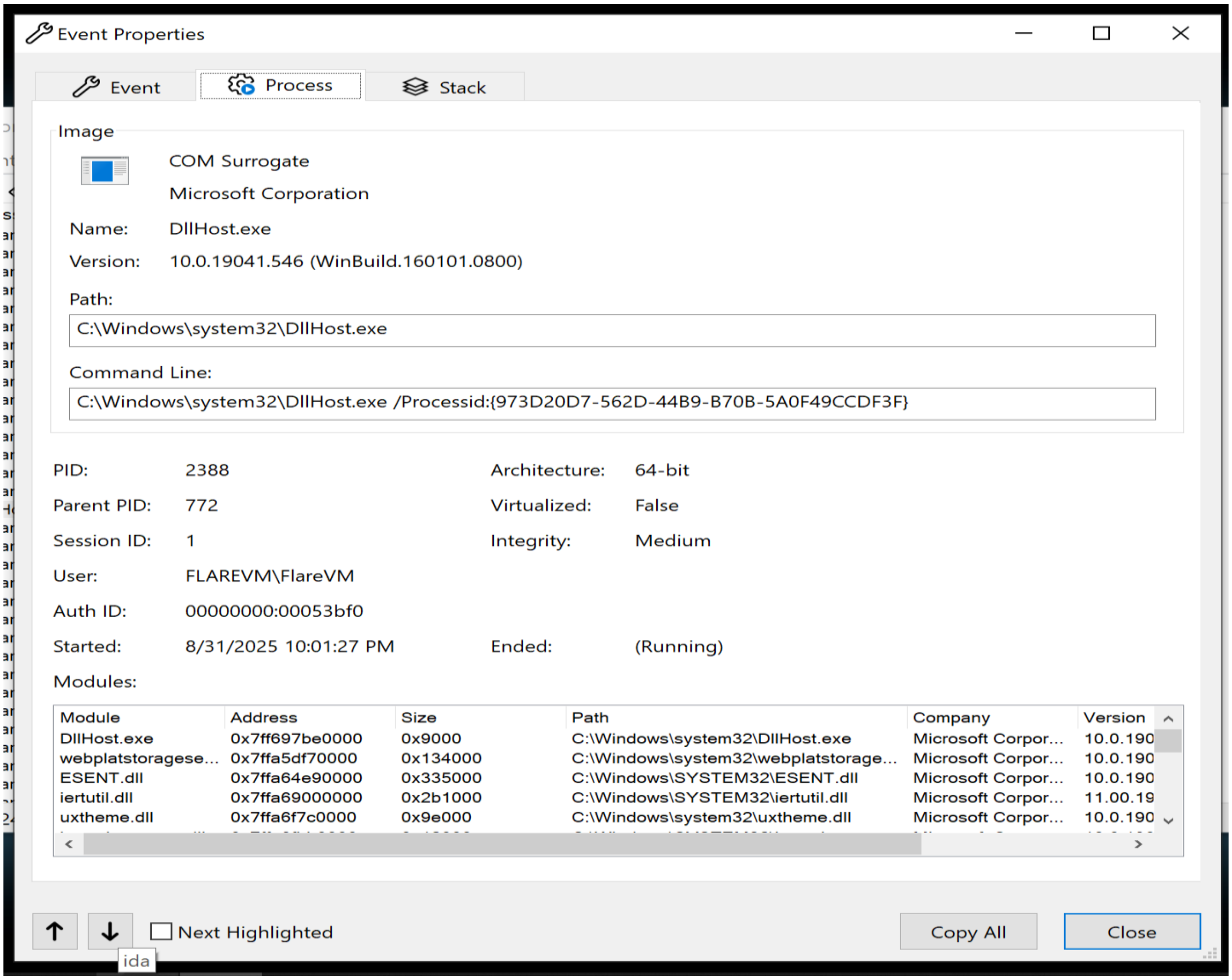
Command: C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A

User: FLAREVM\FlareVM

PID: 5732 Started: 8/31/2025 10:20:43 PM

Exited: 8/31/2025 10:20:48 PM

Event Properties



Image

COM Surrogate

Microsoft Corporation

Name: DllHost.exe

Version: 10.0.19041.546 (WinBuild.160101.0800)

Path:

C:\Windows\system32\DllHost.exe

Command Line:

C:\Windows\system32\DllHost.exe /Processid:{973D20D7-562D-44B9-B70B-5A0F49CCDF3F}

PID: 2388

Architecture: 64-bit

Parent PID: 772

Virtualized: False

Session ID: 1

Integrity: Medium

User: FLAREVM\FlareVM

Auth ID: 00000000:00053bf0

Started: 8/31/2025 10:01:27 PM

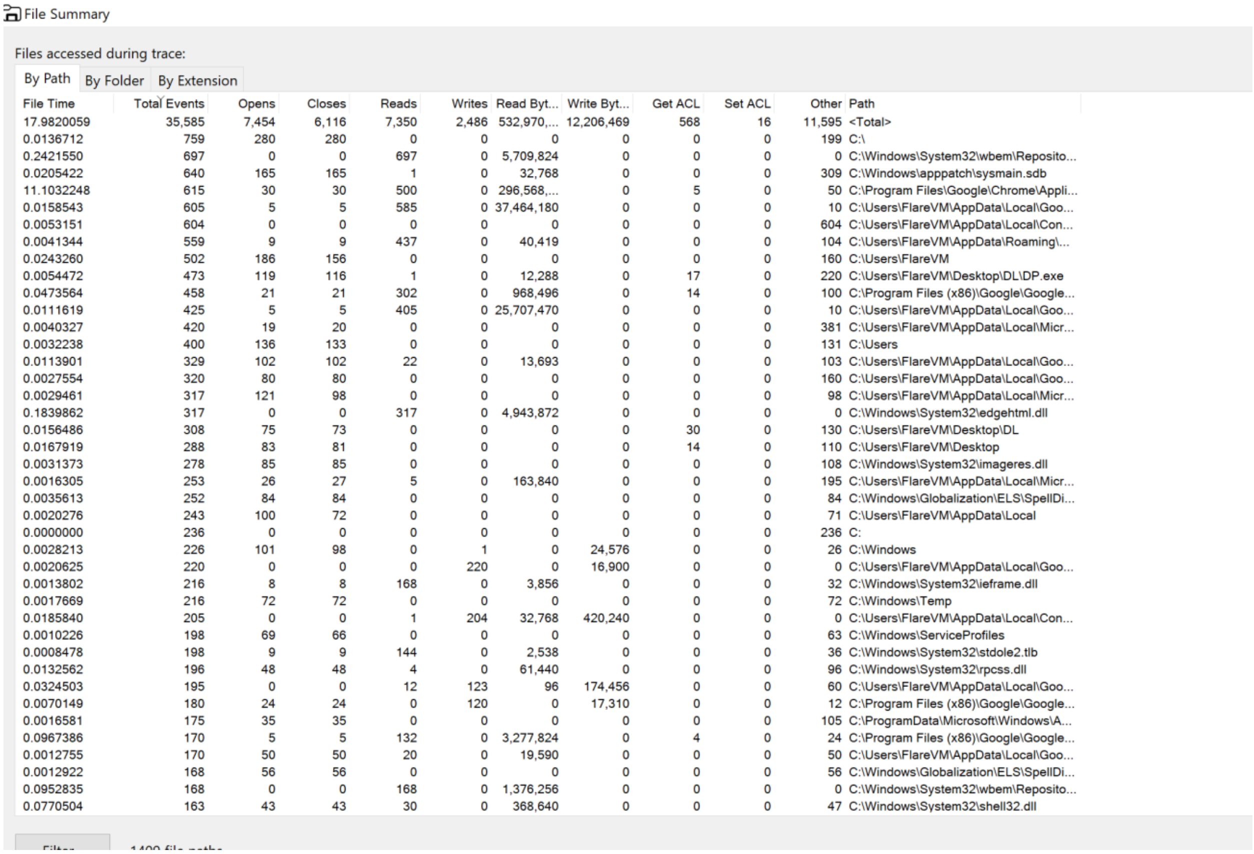
Ended: (Running)

Modules:

Module	Address	Size	Path	Company	Version
DllHost.exe	0x7ff697be0000	0x9000	C:\Windows\system32\DllHost.exe	Microsoft Corpor...	10.0.190
webplatstoragese...	0x7ffa5df70000	0x134000	C:\Windows\system32\webplatstorage...	Microsoft Corpor...	10.0.190
ESENT.dll	0x7ffa64e90000	0x335000	C:\Windows\SYSTEM32\ESENT.dll	Microsoft Corpor...	10.0.190
iertutil.dll	0x7ffa69000000	0x2b1000	C:\Windows\SYSTEM32\iertutil.dll	Microsoft Corpor...	11.00.19
uxtheme.dll	0x7ffa6f7c0000	0x9e000	C:\Windows\system32\uxtheme.dll	Microsoft Corpor...	10.0.190

☐ Next Highlighted

File Summary:

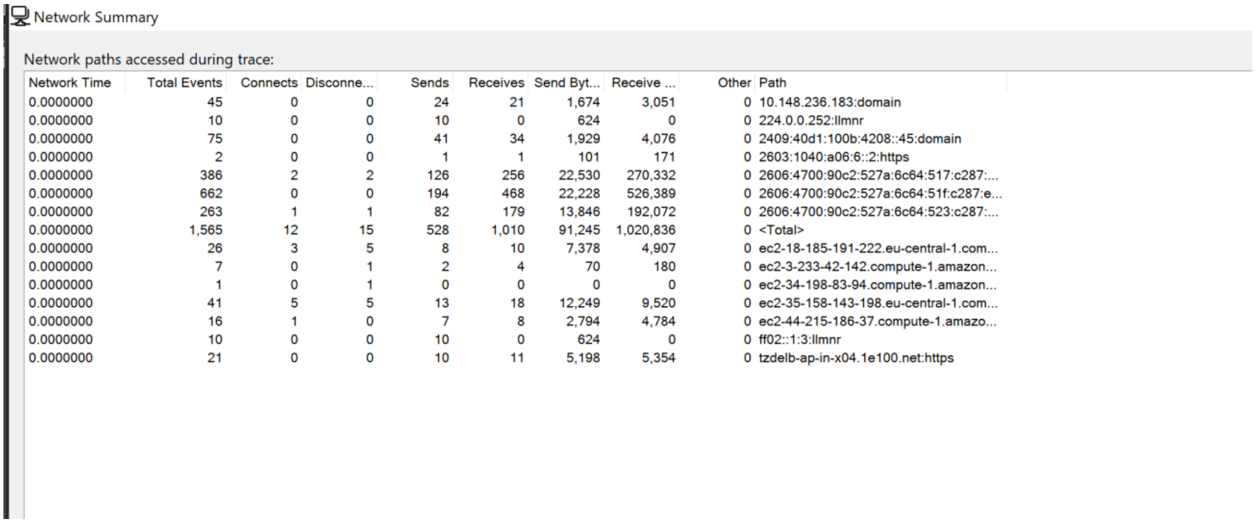


Files accessed during trace:

File Time	Total Events	Opens	Closes	Reads	Writes	Read Byt...	Write Byt...	Get ACL	Set ACL	Other	Path
17.9820059	35,585	7,454	6,116	7,350	2,486	532,970,...	12,206,469	568	16	11,595	<Total>
0.0136712	759	280	280	0	0	0	0	0	0	199	C:\
0.2421550	697	0	0	697	0	5,709,824	0	0	0	0	C:\Windows\System32\wbem\Reposito...
0.0205422	640	165	165	1	0	32,768	0	0	0	309	C:\Windows\apppatch\sysmain.sdb
11.1032248	615	30	30	500	0	296,568,...	0	5	0	50	C:\Program Files\Google\Chrome\Appli...
0.0158543	605	5	5	585	0	37,464,180	0	0	0	10	C:\Users\FlareVM\AppData\Local\Goo...
0.0053151	604	0	0	0	0	0	0	0	0	604	C:\Users\FlareVM\AppData\Local\Con...
0.0041344	559	9	9	437	0	40,419	0	0	0	104	C:\Users\FlareVM\AppData\Roaming\...
0.0243260	502	186	156	0	0	0	0	0	0	160	C:\Users\FlareVM
0.0054472	473	119	116	1	0	12,288	0	17	0	220	C:\Users\FlareVM\Desktop\DL\DP.exe
0.0473564	458	21	21	302	0	968,496	0	14	0	100	C:\Program Files (x86)\Google\Google...
0.0111619	425	5	5	405	0	25,707,470	0	0	0	10	C:\Users\FlareVM\AppData\Local\Goo...
0.0040327	420	19	20	0	0	0	0	0	0	381	C:\Users\FlareVM\AppData\Local\Micr...
0.0032238	400	136	133	0	0	0	0	0	0	131	C:\Users
0.0113901	329	102	102	22	0	13,693	0	0	0	103	C:\Users\FlareVM\AppData\Local\Goo...
0.0027554	320	80	80	0	0	0	0	0	0	160	C:\Users\FlareVM\AppData\Local\Goo...
0.0029461	317	121	98	0	0	0	0	0	0	98	C:\Users\FlareVM\AppData\Local\Micr...
0.1839862	317	0	0	317	0	4,943,872	0	0	0	0	C:\Windows\System32\edgehtml.dll
0.0156486	308	75	73	0	0	0	0	30	0	130	C:\Users\FlareVM\Desktop\DL
0.0167919	288	83	81	0	0	0	0	14	0	110	C:\Users\FlareVM\Desktop
0.0031373	278	85	85	0	0	0	0	0	0	108	C:\Windows\System32\imageres.dll
0.0016305	253	26	27	5	0	163,840	0	0	0	195	C:\Users\FlareVM\AppData\Local\Micr...
0.0035613	252	84	84	0	0	0	0	0	0	84	C:\Windows\Globalization\ELS\SpellDi...
0.0020276	243	100	72	0	0	0	0	0	0	71	C:\Users\FlareVM\AppData\Local
0.0000000	236	0	0	0	0	0	0	0	0	236	C:
0.0028213	226	101	98	0	1	0	24,576	0	0	26	C:\Windows
0.0020625	220	0	0	0	220	0	16,900	0	0	0	C:\Users\FlareVM\AppData\Local\Goo...
0.0013802	216	8	8	168	0	3,856	0	0	0	32	C:\Windows\System32\ieframe.dll
0.0017669	216	72	72	0	0	0	0	0	0	72	C:\Windows\Temp
0.0185840	205	0	0	1	204	32,768	420,240	0	0	0	C:\Users\FlareVM\AppData\Local\Con...
0.0010226	198	69	66	0	0	0	0	0	0	63	C:\Windows\ServiceProfiles
0.0008478	198	9	9	144	0	2,538	0	0	0	36	C:\Windows\System32\stdole2.tlb
0.0132562	196	48	48	4	0	61,440	0	0	0	96	C:\Windows\System32\rpcss.dll
0.0324503	195	0	0	12	123	96	174,456	0	0	60	C:\Users\FlareVM\AppData\Local\Goo...
0.0070149	180	24	24	0	120	0	17,310	0	0	12	C:\Program Files (x86)\Google\Google...
0.0016581	175	35	35	0	0	0	0	0	0	105	C:\ProgramData\Microsoft\Windows\A...
0.0967386	170	5	5	132	0	3,277,824	0	4	0	24	C:\Program Files (x86)\Google\Google...
0.0012755	170	50	50	20	0	19,590	0	0	0	50	C:\Users\FlareVM\AppData\Local\Goo...
0.0012922	168	56	56	0	0	0	0	0	0	56	C:\Windows\Globalization\ELS\SpellDi...
0.0952835	168	0	0	168	0	1,376,256	0	0	0	0	C:\Windows\System32\wbem\Reposito...
0.0770504	163	43	43	30	0	368,640	0	0	0	47	C:\Windows\System32\shell32.dll

1400 file paths

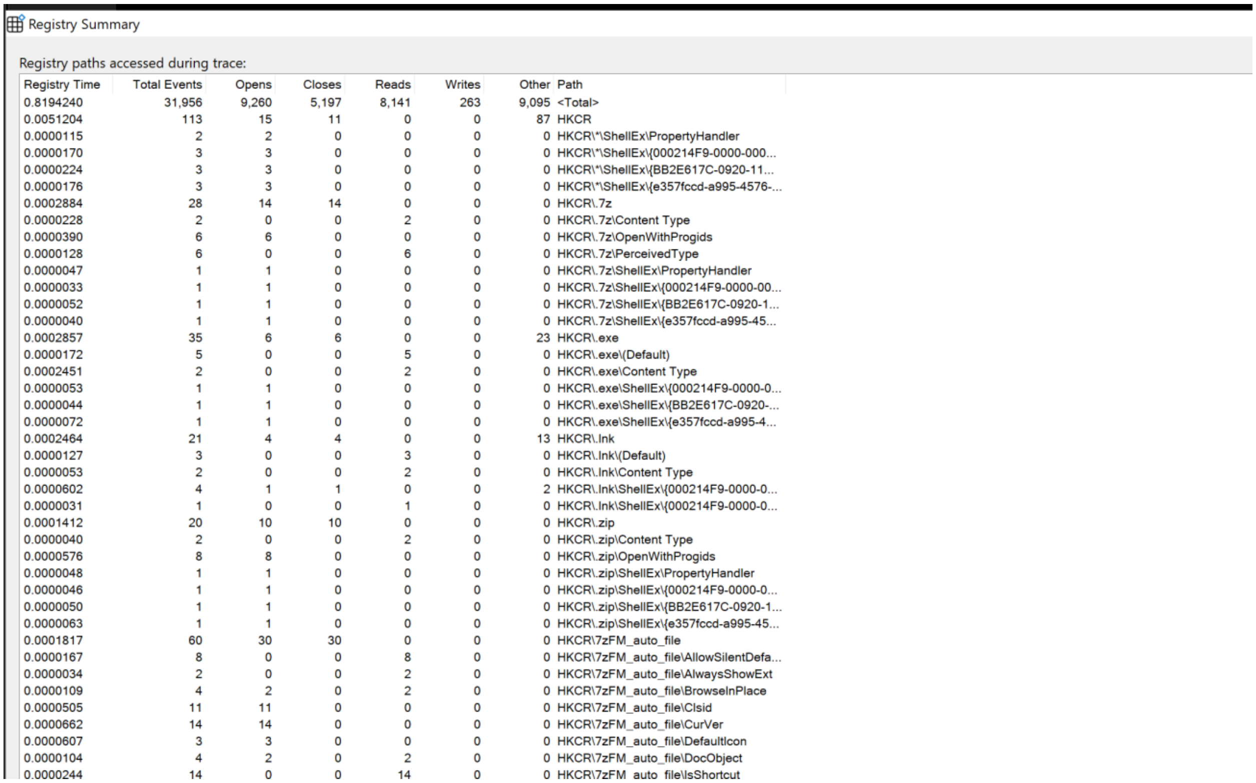
Network Summary:



Network paths accessed during trace:

Network Time	Total Events	Connects	Disconne...	Sends	Receives	Send Byt...	Receive ...	Other	Path
0.0000000	45	0	0	24	21	1,674	3,051	0	10.148.236.183:domain
0.0000000	10	0	0	10	0	624	0	0	224.0.0.252:llmnr
0.0000000	75	0	0	41	34	1,929	4,076	0	2409:40d1:100b:4208::45:domain
0.0000000	2	0	0	1	1	101	171	0	2603:1040:a06:6::2:https
0.0000000	386	2	2	126	256	22,530	270,332	0	2606:4700:90c2:527a:6c64:517:c287:...
0.0000000	662	0	0	194	468	22,228	526,389	0	2606:4700:90c2:527a:6c64:51f:c287:e...
0.0000000	263	1	1	82	179	13,846	192,072	0	2606:4700:90c2:527a:6c64:523:c287:...
0.0000000	1,565	12	15	528	1,010	91,245	1,020,836	0	<Total>
0.0000000	26	3	5	8	10	7,378	4,907	0	ec2-18-185-191-222.eu-central-1.com...
0.0000000	7	0	1	2	4	70	180	0	ec2-3-233-42-142.compute-1.amazon...
0.0000000	1	0	1	0	0	0	0	0	ec2-34-198-83-94.compute-1.amazon...
0.0000000	41	5	5	13	18	12,249	9,520	0	ec2-35-158-143-198.eu-central-1.com...
0.0000000	16	1	0	7	8	2,794	4,784	0	ec2-44-215-186-37.compute-1.amazo...
0.0000000	10	0	0	10	0	624	0	0	ff02::1:3:llmnr
0.0000000	21	0	0	10	11	5,198	5,354	0	tzdelb-ap-in-x04.1e100.net:https

Registry Summary:



Registry Summary

Registry paths accessed during trace:

Registry Time	Total Events	Opens	Closes	Reads	Writes	Other	Path
0.8194240	31,956	9,260	5,197	8,141	263	9,095	<Total>
0.0051204	113	15	11	0	0	87	HKCR
0.0000115	2	2	0	0	0	0	HKCR*\ShellEx\PropertyHandler
0.0000170	3	3	0	0	0	0	HKCR*\ShellEx\{000214F9-0000-000...
0.0000224	3	3	0	0	0	0	HKCR*\ShellEx\{BB2E617C-0920-11...
0.0000176	3	3	0	0	0	0	HKCR*\ShellEx\{e357fccd-a995-4576-...
0.0002884	28	14	14	0	0	0	HKCR\.7z
0.0000228	2	0	0	2	0	0	HKCR\.7z\Content Type
0.0000390	6	6	0	0	0	0	HKCR\.7z\OpenWithProgids
0.0000128	6	0	0	6	0	0	HKCR\.7z\PerceivedType
0.0000047	1	1	0	0	0	0	HKCR\.7z\ShellEx\PropertyHandler
0.0000033	1	1	0	0	0	0	HKCR\.7z\ShellEx\{000214F9-0000-00...
0.0000052	1	1	0	0	0	0	HKCR\.7z\ShellEx\{BB2E617C-0920-1...
0.0000040	1	1	0	0	0	0	HKCR\.7z\ShellEx\{e357fccd-a995-45...
0.0002857	35	6	6	0	0	23	HKCR\.exe
0.0000172	5	0	0	5	0	0	HKCR\.exe\(Default)
0.0002451	2	0	0	2	0	0	HKCR\.exe\Content Type
0.0000053	1	1	0	0	0	0	HKCR\.exe\ShellEx\{000214F9-0000-0...
0.0000044	1	1	0	0	0	0	HKCR\.exe\ShellEx\{BB2E617C-0920-...
0.0000072	1	1	0	0	0	0	HKCR\.exe\ShellEx\{e357fccd-a995-4...
0.0002464	21	4	4	0	0	13	HKCR\.lnk
0.0000127	3	0	0	3	0	0	HKCR\.lnk\(Default)
0.0000053	2	0	0	2	0	0	HKCR\.lnk\Content Type
0.0000602	4	1	1	0	0	2	HKCR\.lnk\ShellEx\{000214F9-0000-0...
0.0000031	1	0	0	1	0	0	HKCR\.lnk\ShellEx\{000214F9-0000-0...
0.0001412	20	10	10	0	0	0	HKCR\.zip
0.0000040	2	0	0	2	0	0	HKCR\.zip\Content Type
0.0000576	8	8	0	0	0	0	HKCR\.zip\OpenWithProgids
0.0000048	1	1	0	0	0	0	HKCR\.zip\ShellEx\PropertyHandler
0.0000046	1	1	0	0	0	0	HKCR\.zip\ShellEx\{000214F9-0000-0...
0.0000050	1	1	0	0	0	0	HKCR\.zip\ShellEx\{BB2E617C-0920-1...
0.0000063	1	1	0	0	0	0	HKCR\.zip\ShellEx\{e357fccd-a995-45...
0.0001817	60	30	30	0	0	0	HKCR\7zFM_auto_file
0.0000167	8	0	0	8	0	0	HKCR\7zFM_auto_file\AllowSilentDefa...
0.0000034	2	0	0	2	0	0	HKCR\7zFM_auto_file\AlwaysShowExt
0.0000109	4	2	0	2	0	0	HKCR\7zFM_auto_file\BrowseInPlace
0.0000505	11	11	0	0	0	0	HKCR\7zFM_auto_file\Clsid
0.0000662	14	14	0	0	0	0	HKCR\7zFM_auto_file\CurVer
0.0000607	3	3	0	0	0	0	HKCR\7zFM_auto_file\DefaultIcon
0.0000104	4	2	0	2	0	0	HKCR\7zFM_auto_file\DocObject
0.0000244	14	0	0	14	0	0	HKCR\7zFM_auto_file\IsShortcut

Document Analysis

1. **File Hashes**
   - MD5: 1d8562c0adcaee734d63f7baaca02f7c

2. **Suspicious Strings & Commands**
   - cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
   - ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe
3. **Payload Path**
   - C:\Users\Public\Documents\CR433101.dat.exe
4. **Network Indicators**
   - http://ssl-6582datamanager.helpdeskbros.local/favicon.ico
   - http://huskyhacks.dev
   - Mozilla/5.0 (User-Agent for disguise)
5. **API Calls**
   - URLDownloadToFileW, InternetOpenUrlW, InternetOpenW → downloading payloads.
   - ShellExecuteW, CreateProcessW → executing payloads.
   - IsDebuggerPresent, QueryPerformanceCounter → anti-debugging checks.

Malware Behaviour: Downloads payloads, executes them, deletes traces, uses sleep tricks**.**

Persistence: Not directly observed in logs, but secondary payload (CR433101.dat.exe) likely sets persistence.