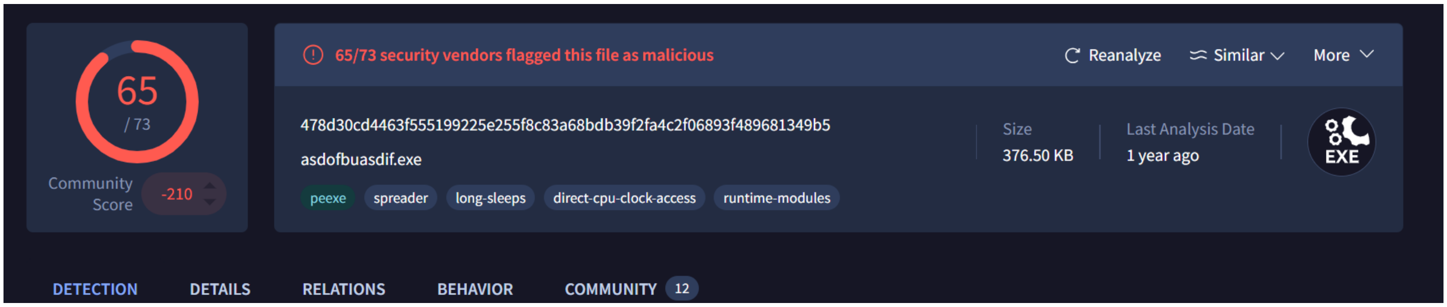
Name:Samiksha Patil

Intern ID:280

Malware Analysis Report

Malware Tool: : W32.VBS_DufakaDGH.Trojan

Hash Value:(SHA-256): 478d30cd4463f555199225e2558c83a68bdb39f2fa4c2f06893f489681349b



65/73 security vendors flagged this file as malicious

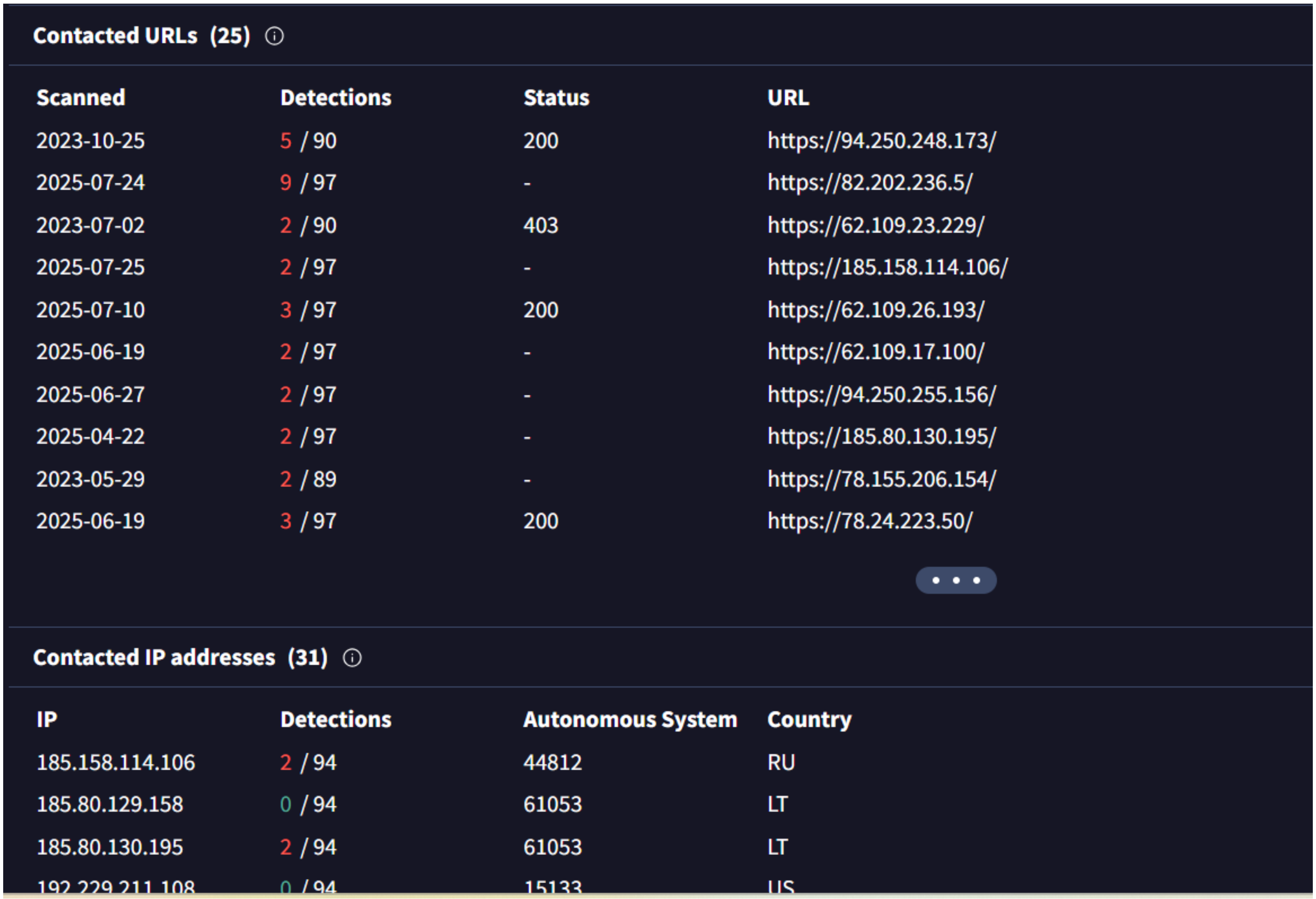
478d30cd4463f555199225e255f8c83a68bdb39f2fa4c2f06893f489681349b5

asdofbuasdif.exe

peexe spreader long-sleeps direct-cpu-clock-access runtime-modules

Size 376.50 KB

Last Analysis Date 1 year ago

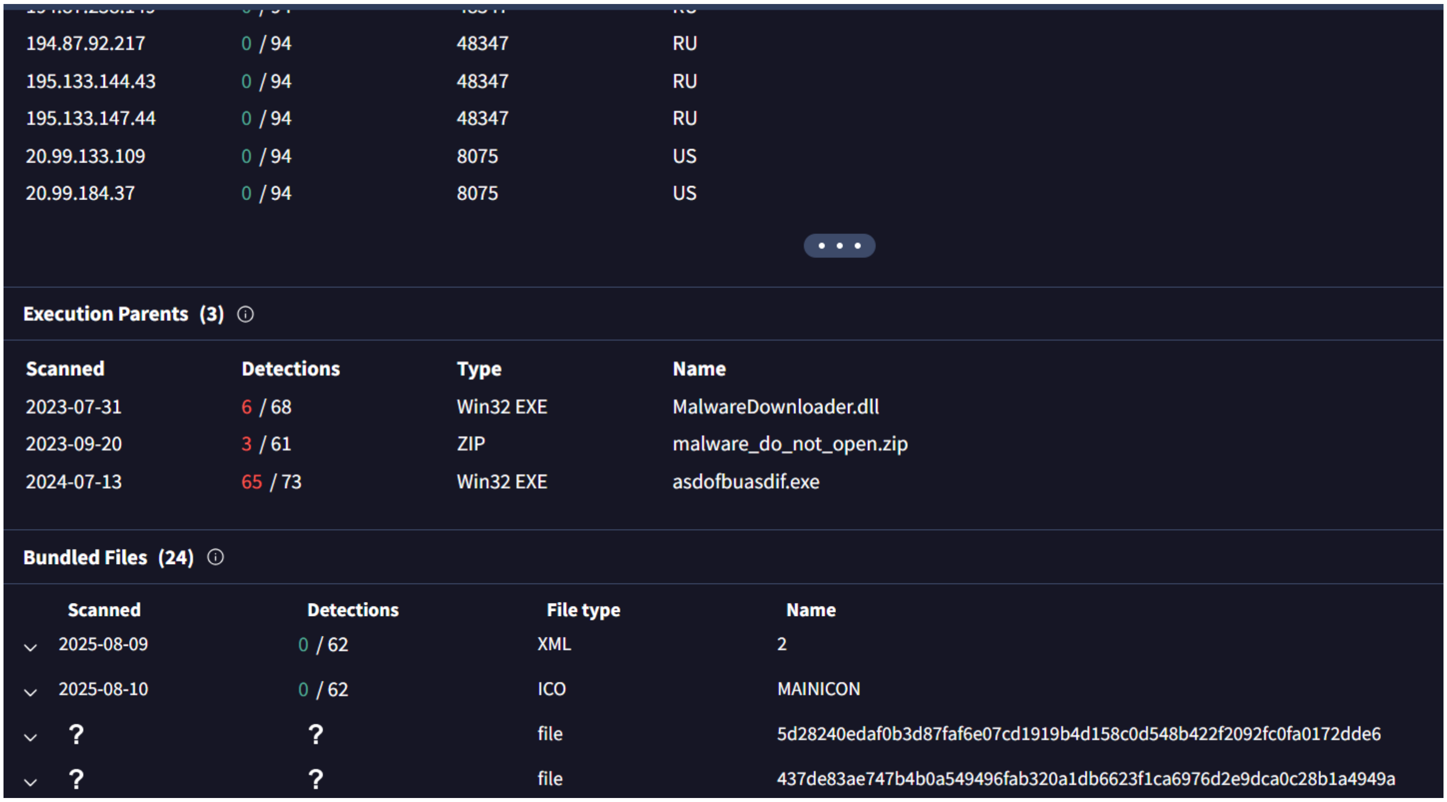


Contacted URLs (25)

Scanned	Detections	Status	URL
2023-10-25	5 / 90	200	https://94.250.248.173/
2025-07-24	9 / 97	-	https://82.202.236.5/
2023-07-02	2 / 90	403	https://62.109.23.229/
2025-07-25	2 / 97	-	https://185.158.114.106/
2025-07-10	3 / 97	200	https://62.109.26.193/
2025-06-19	2 / 97	-	https://62.109.17.100/
2025-06-27	2 / 97	-	https://94.250.255.156/
2025-04-22	2 / 97	-	https://185.80.130.195/
2023-05-29	2 / 89	-	https://78.155.206.154/
2025-06-19	3 / 97	200	https://78.24.223.50/

Contacted IP addresses (31)

IP	Detections	Autonomous System	Country
185.158.114.106	2 / 94	44812	RU
185.80.129.158	0 / 94	61053	LT
185.80.130.195	2 / 94	61053	LT
192.229.211.108	0 / 94	15133	US



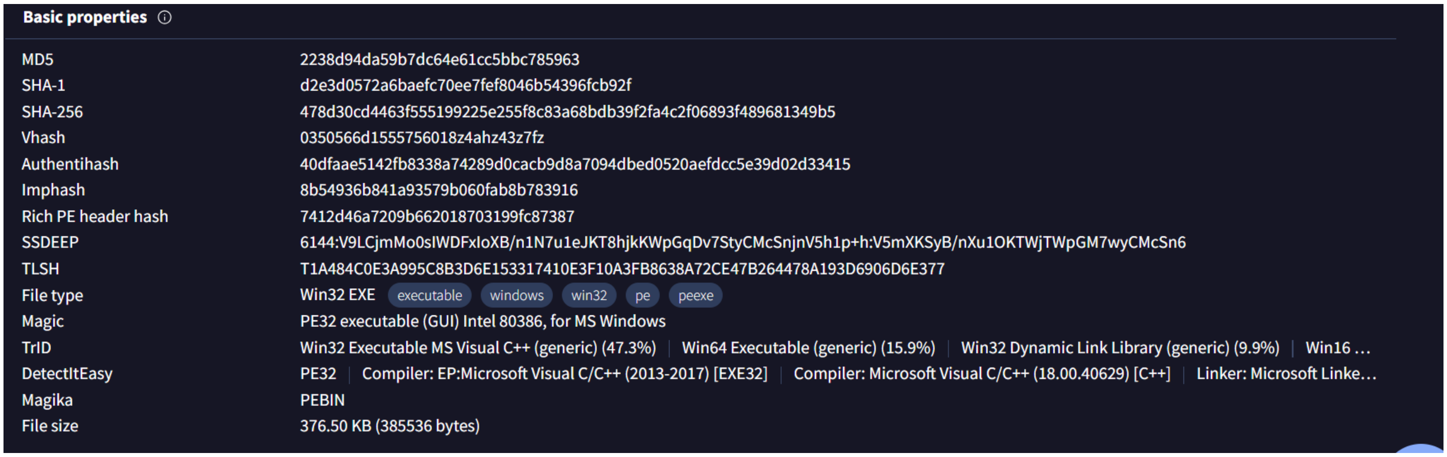
194.87.92.217	0 / 94	48347	RU
195.133.144.43	0 / 94	48347	RU
195.133.147.44	0 / 94	48347	RU
20.99.133.109	0 / 94	8075	US
20.99.184.37	0 / 94	8075	US

Execution Parents (3)

Scanned	Detections	Type	Name
2023-07-31	6 / 68	Win32 EXE	MalwareDownloader.dll
2023-09-20	3 / 61	ZIP	malware_do_not_open.zip
2024-07-13	65 / 73	Win32 EXE	asdofbuasdif.exe

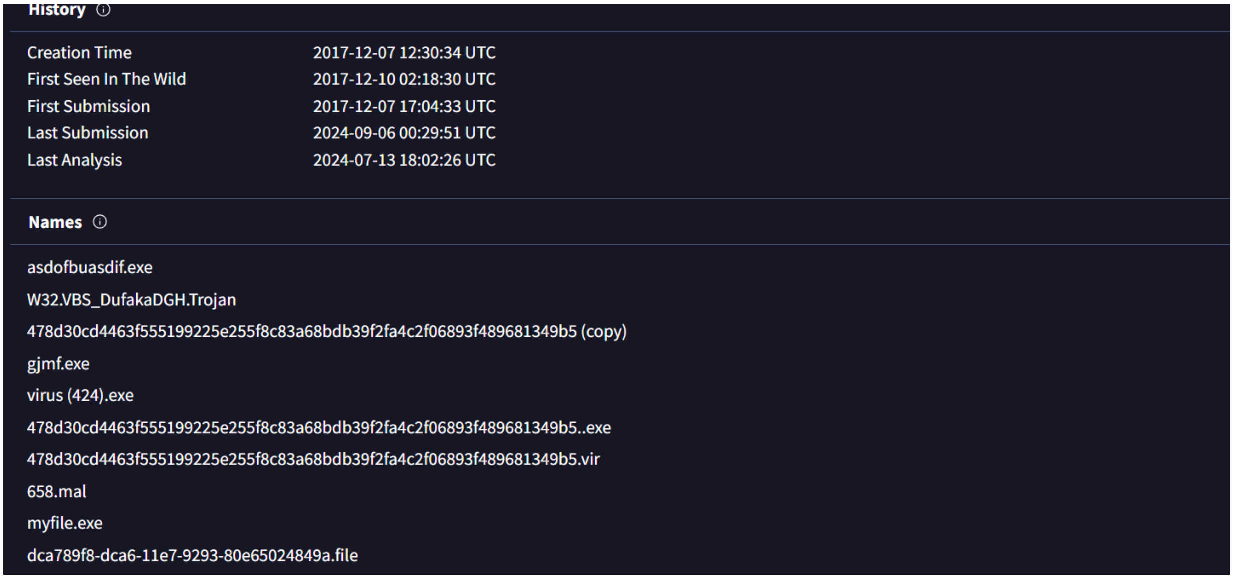
Bundled Files (24)

Scanned	Detections	File type	Name
2025-08-09	0 / 62	XML	2
2025-08-10	0 / 62	ICO	MAINICON
?	?	file	5d28240edaf0b3d87faf6e07cd1919b4d158c0d548b422f2092fc0fa0172dde6
?	?	file	437de83ae747b4b0a549496fab320a1db6623f1ca6976d2e9dca0c28b1a4949a



Basic properties

MD5	2238d94da59b7dc64e61cc5bbc785963
SHA-1	d2e3d0572a6baefc70ee7fef8046b54396fcb92f
SHA-256	478d30cd4463f555199225e255f8c83a68bdb39f2fa4c2f06893f489681349b5
Vhash	0350566d1555756018z4ahz43z7fz
Authentihash	40dfaae5142fb8338a74289d0cacb9d8a7094dbed0520aefdcc5e39d02d33415
Imphash	8b54936b841a93579b060fab8b783916
Rich PE header hash	7412d46a7209b662018703199fc87387
SSDEEP	6144:V9LCjmMo0sIWDFxIoXB/n1N7u1eJKT8hjkKWpGqDv7StyCMcSnjnV5h1p+h:V5mXKSyB/nXu1OKTWjTWpGM7wyCMcSn6
TLSH	T1A484C0E3A995C8B3D6E153317410E3F10A3FB8638A72CE47B264478A193D6906D6E377
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (47.3%) | Win64 Executable (generic) (15.9%) | Win32 Dynamic Link Library (generic) (9.9%) | Win16 …
DetectItEasy	PE32 | Compiler: EP:Microsoft Visual C/C++ (2013-2017) [EXE32] | Compiler: Microsoft Visual C/C++ (18.00.40629) [C++] | Linker: Microsoft Linke…
Magika	PEBIN
File size	376.50 KB (385536 bytes)

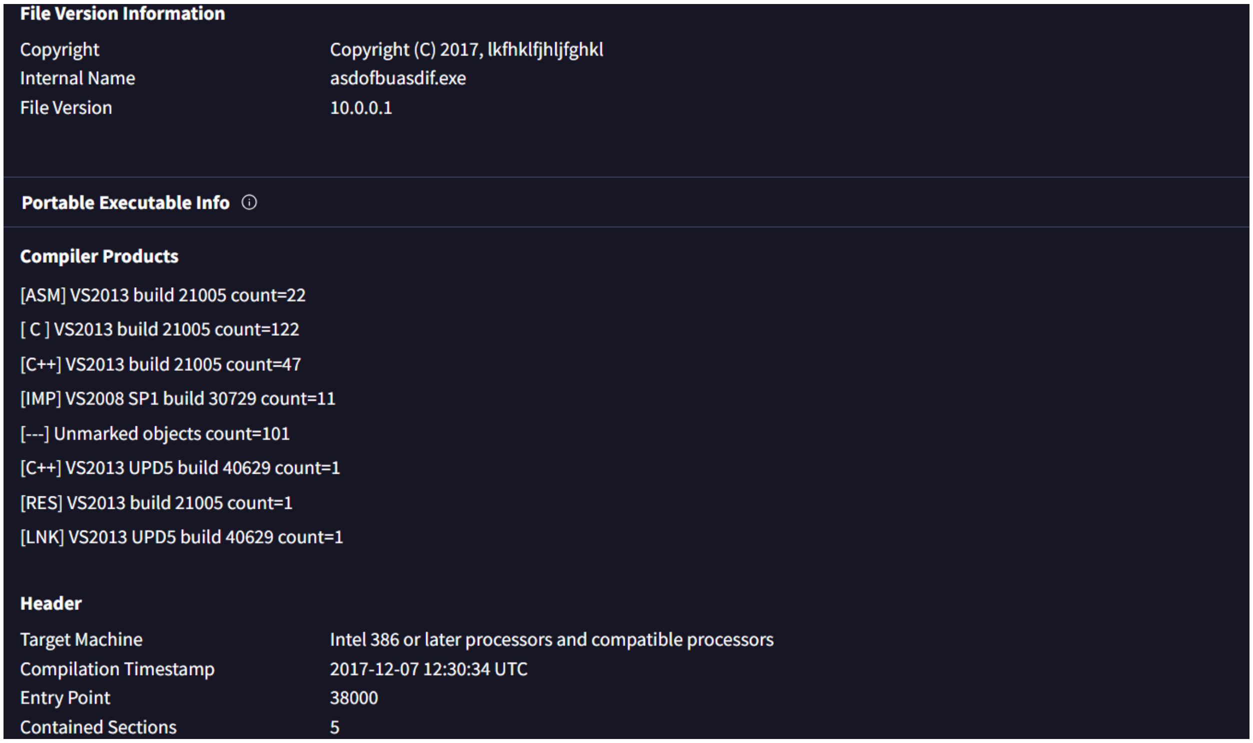


History

Creation Time	2017-12-07 12:30:34 UTC
First Seen In The Wild	2017-12-10 02:18:30 UTC
First Submission	2017-12-07 17:04:33 UTC
Last Submission	2024-09-06 00:29:51 UTC
Last Analysis	2024-07-13 18:02:26 UTC

Names

asdofbuasdif.exe
W32.VBS_DufakaDGH.Trojan
478d30cd4463f555199225e255f8c83a68bdb39f2fa4c2f06893f489681349b5 (copy)
gjmf.exe
virus (424).exe
478d30cd4463f555199225e255f8c83a68bdb39f2fa4c2f06893f489681349b5..exe
478d30cd4463f555199225e255f8c83a68bdb39f2fa4c2f06893f489681349b5.vir
658.mal
myfile.exe
dca789f8-dca6-11e7-9293-80e65024849a.file



File Version Information

Copyright	Copyright (C) 2017, lkfhklfjhljfghkl
Internal Name	asdofbuasdif.exe
File Version	10.0.0.1

Portable Executable Info

Compiler Products

[ASM] VS2013 build 21005 count=22

[C] VS2013 build 21005 count=122

[C++] VS2013 build 21005 count=47

[IMP] VS2008 SP1 build 30729 count=11

[---] Unmarked objects count=101

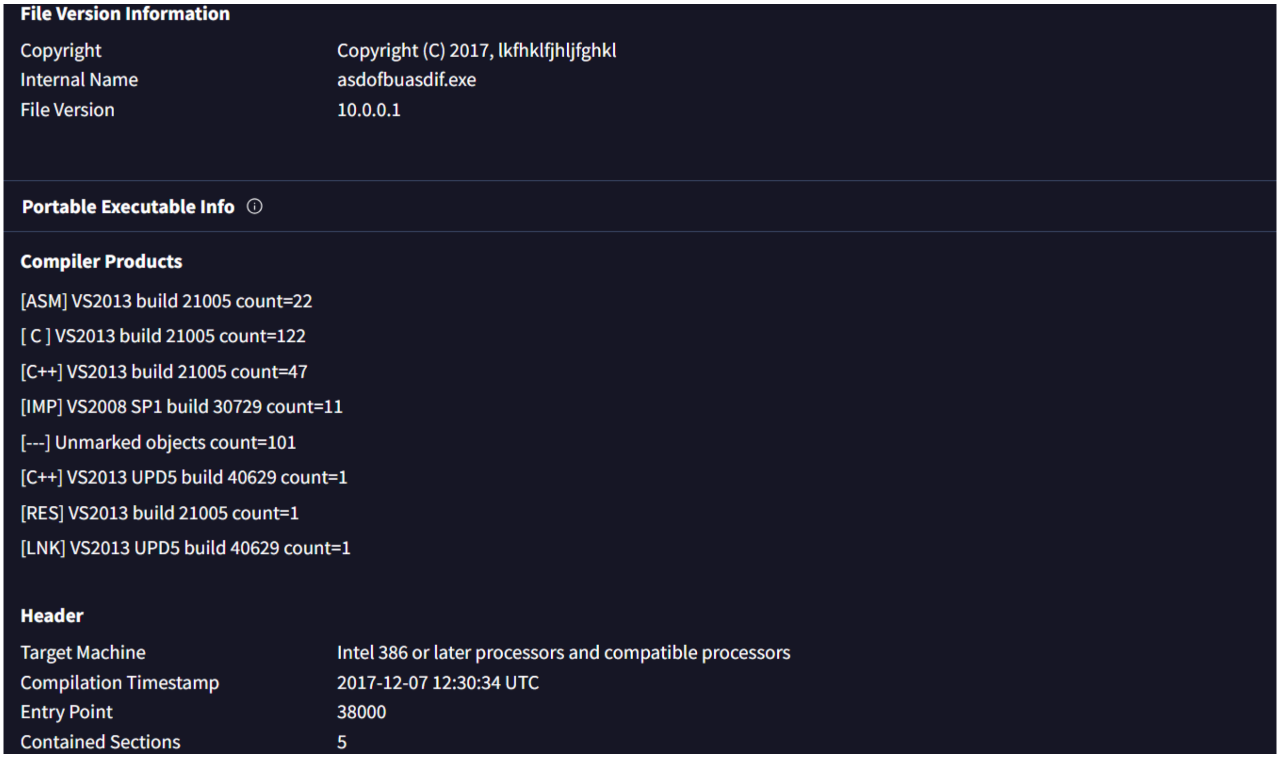
[C++] VS2013 UPD5 build 40629 count=1

[RES] VS2013 build 21005 count=1

[LNK] VS2013 UPD5 build 40629 count=1

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2017-12-07 12:30:34 UTC
Entry Point	38000
Contained Sections	5



File Version Information

Copyright	Copyright (C) 2017, lkfhklfjhljfghkl
Internal Name	asdofbuasdif.exe
File Version	10.0.0.1

Portable Executable Info

Compiler Products

[ASM] VS2013 build 21005 count=22

[C] VS2013 build 21005 count=122

[C++] VS2013 build 21005 count=47

[IMP] VS2008 SP1 build 30729 count=11

[---] Unmarked objects count=101

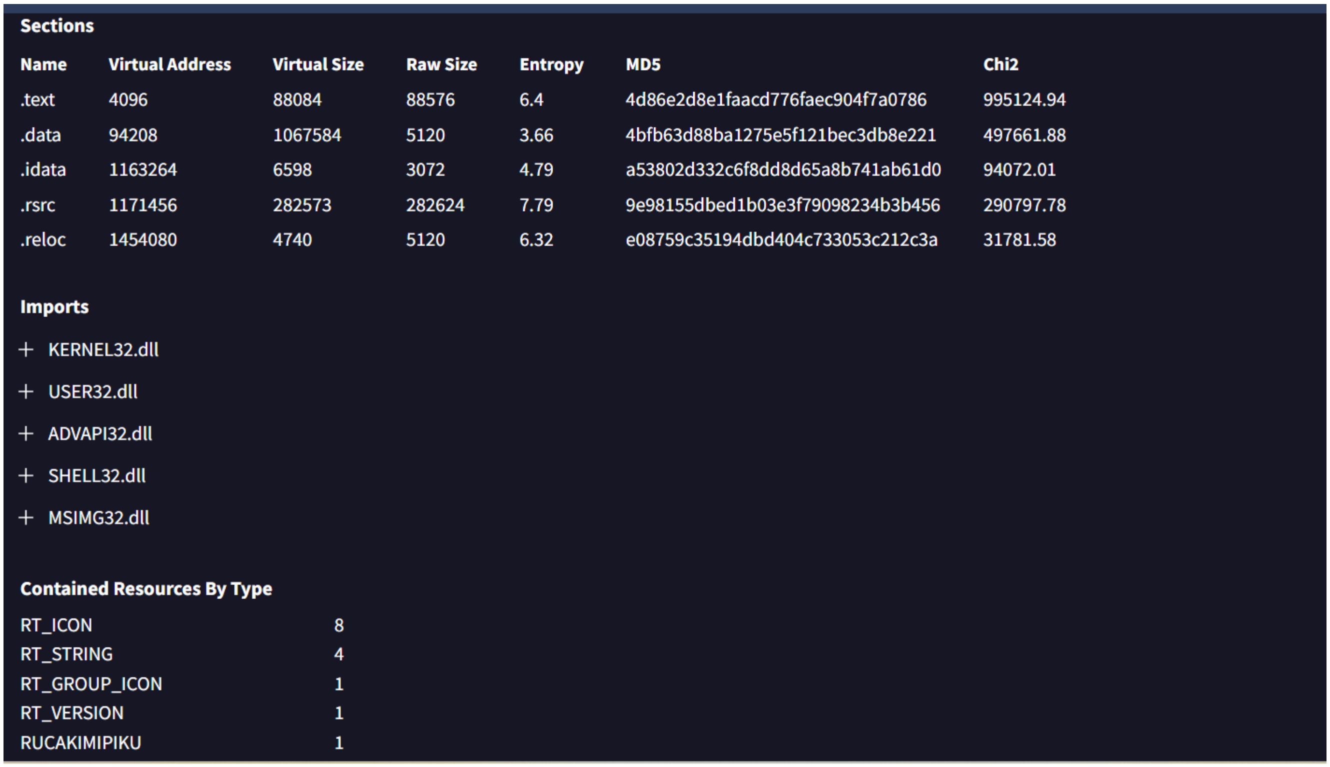
[C++] VS2013 UPD5 build 40629 count=1

[RES] VS2013 build 21005 count=1

[LNK] VS2013 UPD5 build 40629 count=1

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2017-12-07 12:30:34 UTC
Entry Point	38000
Contained Sections	5



Sections

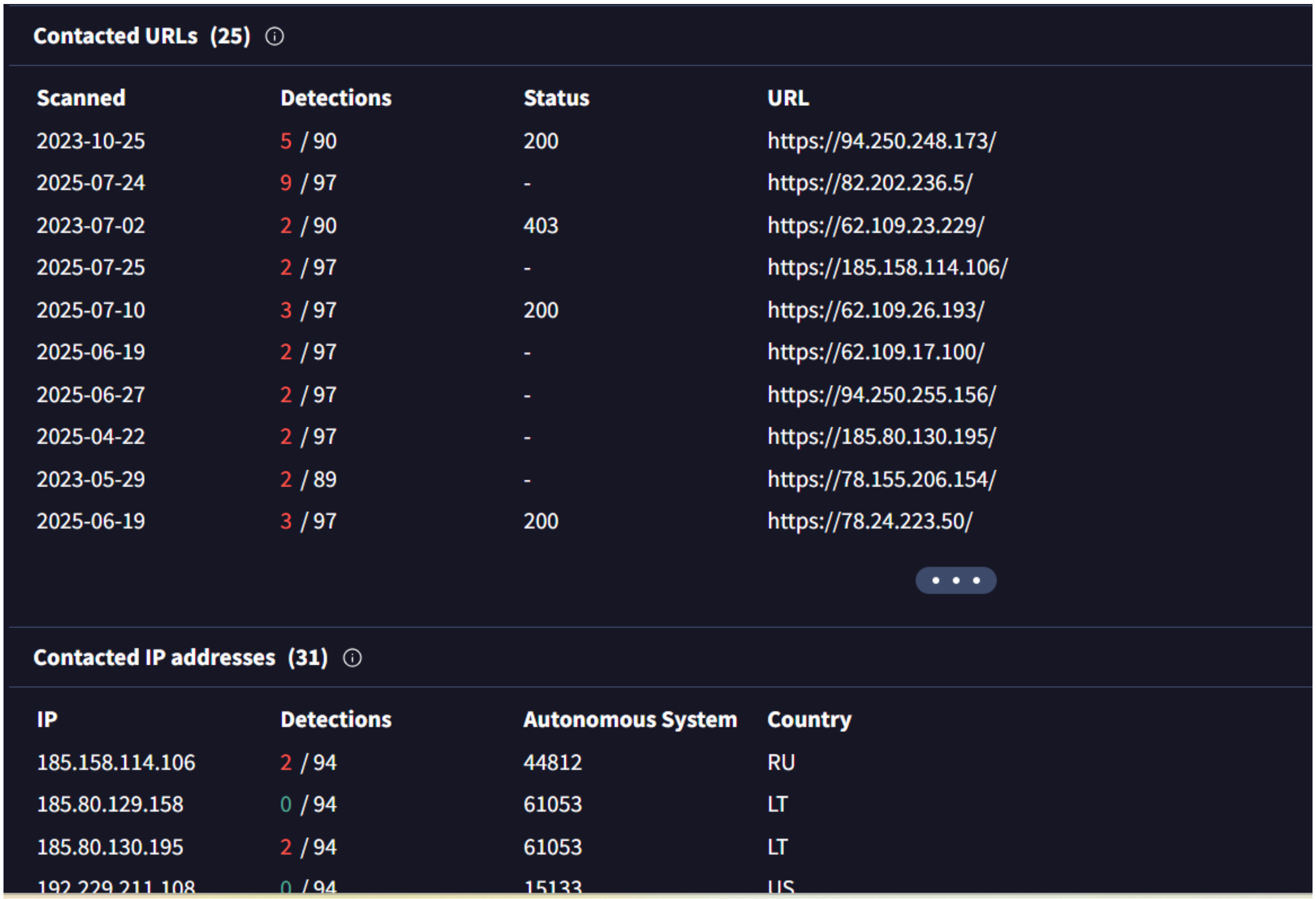
Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	88084	88576	6.4	4d86e2d8e1faacd776faec904f7a0786	995124.94
.data	94208	1067584	5120	3.66	4bfb63d88ba1275e5f121bec3db8e221	497661.88
.idata	1163264	6598	3072	4.79	a53802d332c6f8dd8d65a8b741ab61d0	94072.01
.rsrc	1171456	282573	282624	7.79	9e98155dbed1b03e3f79098234b3b456	290797.78
.reloc	1454080	4740	5120	6.32	e08759c35194dbd404c733053c212c3a	31781.58

Imports

+ KERNEL32.dll
+ USER32.dll
+ ADVAPI32.dll
+ SHELL32.dll
+ MSIMG32.dll

Contained Resources By Type

RT_ICON	8
RT_STRING	4
RT_GROUP_ICON	1
RT_VERSION	1
RUCAKIMIPIKU	1



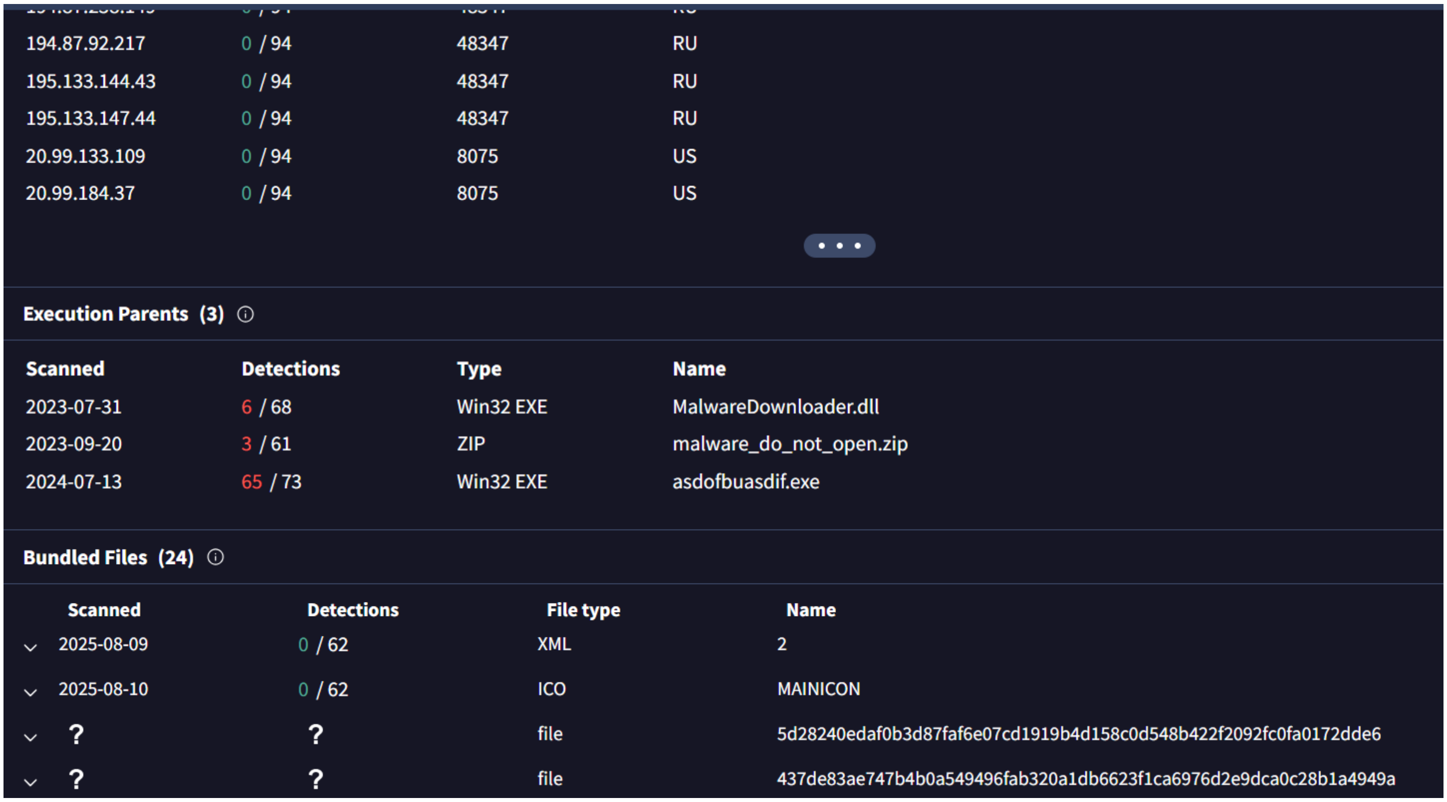
Contacted URLs (25) ⓘ

Scanned	Detections	Status	URL
2023-10-25	5 / 90	200	https://94.250.248.173/
2025-07-24	9 / 97	-	https://82.202.236.5/
2023-07-02	2 / 90	403	https://62.109.23.229/
2025-07-25	2 / 97	-	https://185.158.114.106/
2025-07-10	3 / 97	200	https://62.109.26.193/
2025-06-19	2 / 97	-	https://62.109.17.100/
2025-06-27	2 / 97	-	https://94.250.255.156/
2025-04-22	2 / 97	-	https://185.80.130.195/
2023-05-29	2 / 89	-	https://78.155.206.154/
2025-06-19	3 / 97	200	https://78.24.223.50/

• • •

Contacted IP addresses (31) ⓘ

IP	Detections	Autonomous System	Country
185.158.114.106	2 / 94	44812	RU
185.80.129.158	0 / 94	61053	LT
185.80.130.195	2 / 94	61053	LT
192.229.211.108	0 / 94	15133	US



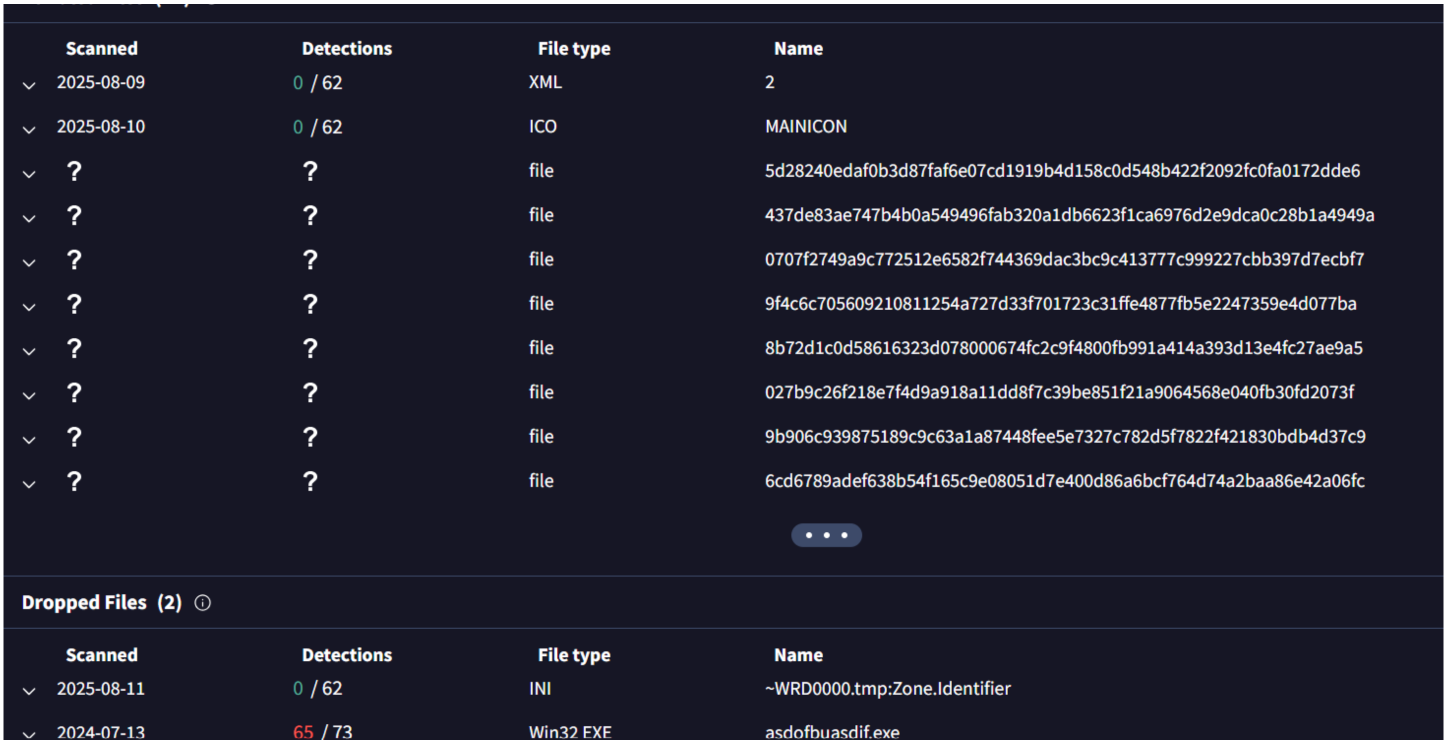
194.87.92.217	0 / 94	48347	RU
195.133.144.43	0 / 94	48347	RU
195.133.147.44	0 / 94	48347	RU
20.99.133.109	0 / 94	8075	US
20.99.184.37	0 / 94	8075	US

Execution Parents (3)

Scanned	Detections	Type	Name
2023-07-31	6 / 68	Win32 EXE	MalwareDownloader.dll
2023-09-20	3 / 61	ZIP	malware_do_not_open.zip
2024-07-13	65 / 73	Win32 EXE	asdofbuasdif.exe

Bundled Files (24)

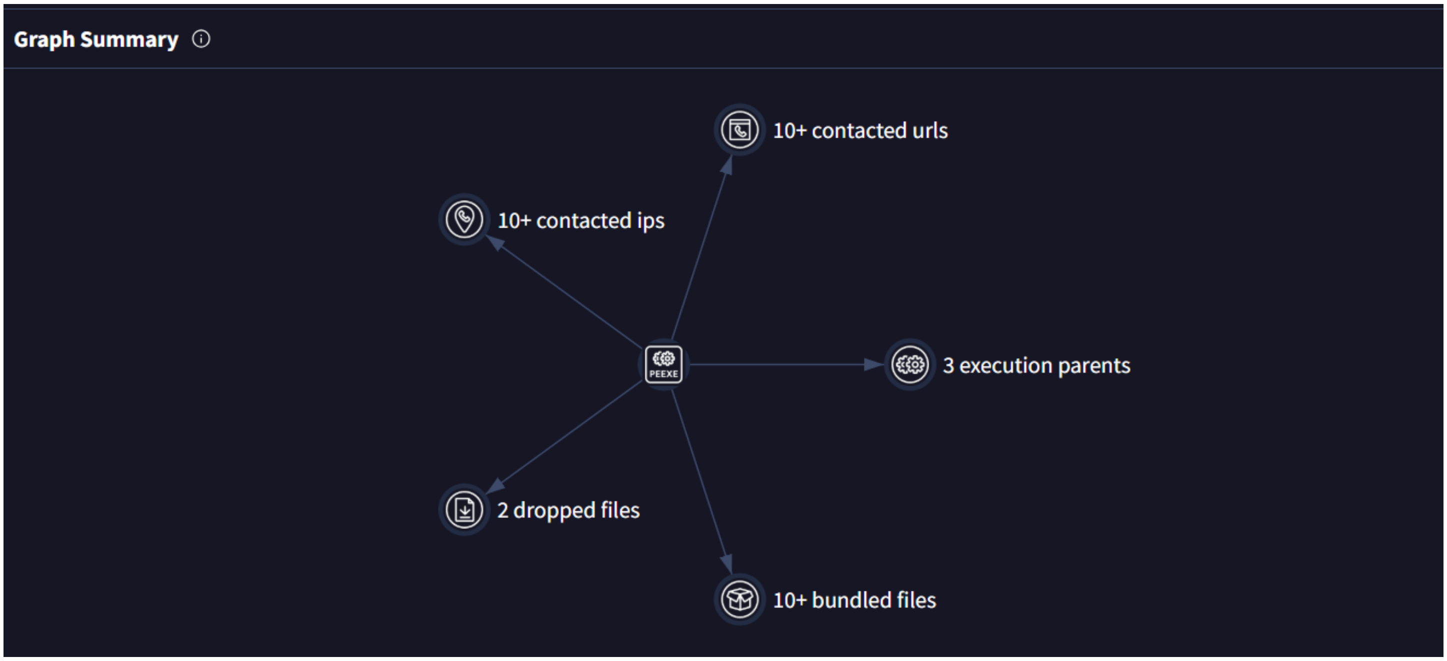
Scanned	Detections	File type	Name
2025-08-09	0 / 62	XML	2
2025-08-10	0 / 62	ICO	MAINICON
?	?	file	5d28240edaf0b3d87faf6e07cd1919b4d158c0d548b422f2092fc0fa0172dde6
?	?	file	437de83ae747b4b0a549496fab320a1db6623f1ca6976d2e9dca0c28b1a4949a

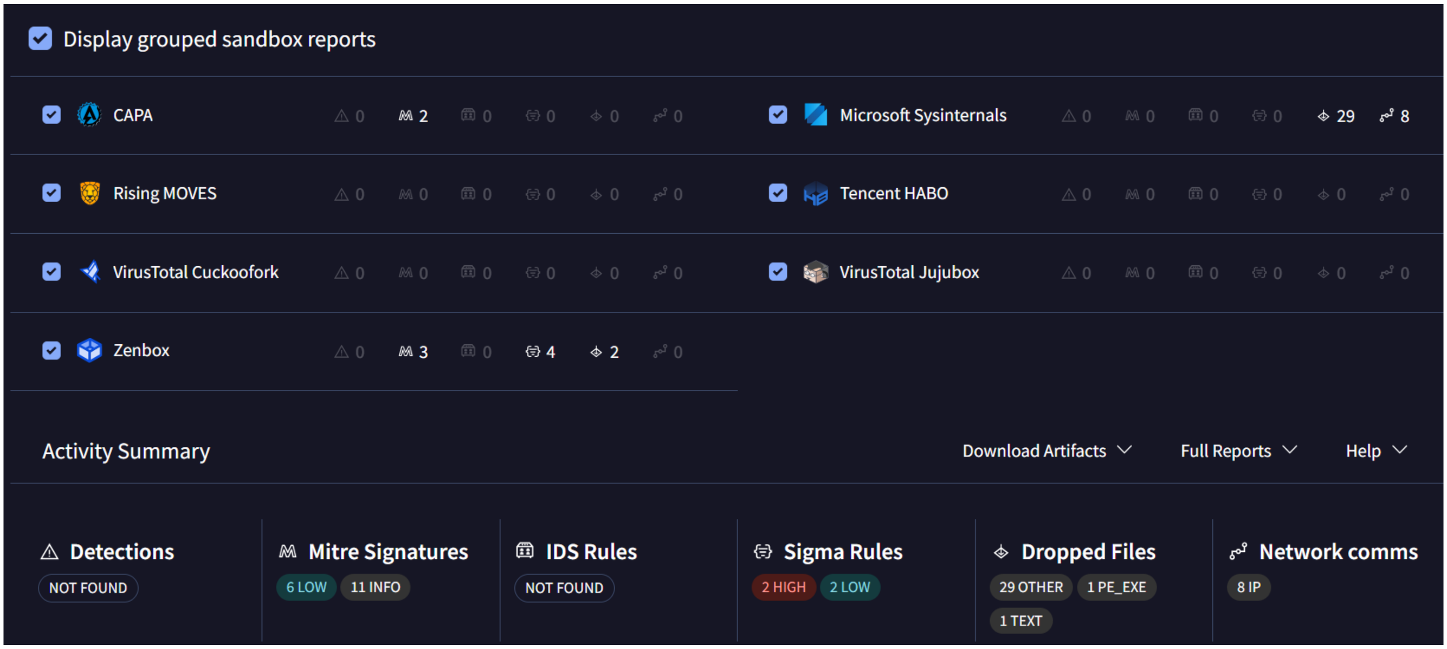


Scanned	Detections	File type	Name
2025-08-09	0 / 62	XML	2
2025-08-10	0 / 62	ICO	MAINICON
?	?	file	5d28240edaf0b3d87faf6e07cd1919b4d158c0d548b422f2092fc0fa0172dde6
?	?	file	437de83ae747b4b0a549496fab320a1db6623f1ca6976d2e9dca0c28b1a4949a
?	?	file	0707f2749a9c772512e6582f744369dac3bc9c413777c999227cbb397d7ecbf7
?	?	file	9f4c6c705609210811254a727d33f701723c31ffe4877fb5e2247359e4d077ba
?	?	file	8b72d1c0d58616323d078000674fc2c9f4800fb991a414a393d13e4fc27ae9a5
?	?	file	027b9c26f218e7f4d9a918a11dd8f7c39be851f21a9064568e040fb30fd2073f
?	?	file	9b906c939875189c9c63a1a87448fee5e7327c782d5f7822f421830bdb4d37c9
?	?	file	6cd6789adef638b54f165c9e08051d7e400d86a6bcf764d74a2baa86e42a06fc

Dropped Files (2)

Scanned	Detections	File type	Name
2025-08-11	0 / 62	INI	~WRD0000.tmp:Zone.Identifier
2024-07-13	65 / 73	Win32 EXE	asdofbuasdif.exe





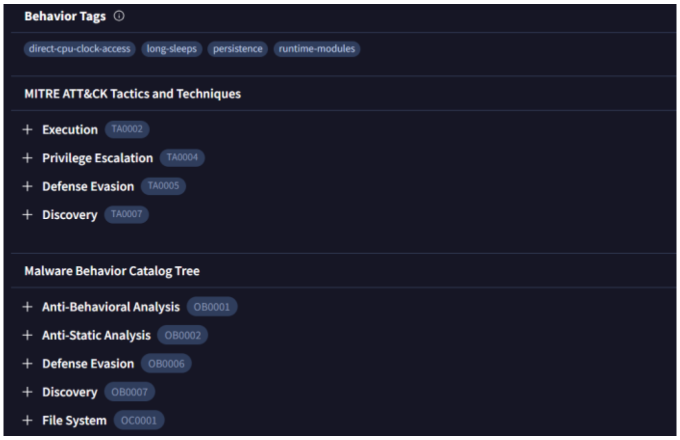
☑ Display grouped sandbox reports

☑	CAPA	⚠ 0	2	0	0	0	0	☑	Microsoft Sysinternals	⚠ 0	0	0	0	29	8
☑	Rising MOVES	⚠ 0	0	0	0	0	0	☑	Tencent HABO	⚠ 0	0	0	0	0	0
☑	VirusTotal Cuckoofork	⚠ 0	0	0	0	0	0	☑	VirusTotal Jujubox	⚠ 0	0	0	0	0	0
☑	Zenbox	⚠ 0	3	0	4	2	0								

Activity Summary

Download Artifacts ⌄ Full Reports ⌄ Help ⌄

⚠ Detections	Mitre Signatures	IDS Rules	Sigma Rules	Dropped Files	Network comms
NOT FOUND	6 LOW 11 INFO	NOT FOUND	2 HIGH 2 LOW	29 OTHER 1 PE_EXE 1 TEXT	8 IP



Behavior Tags ⓘ

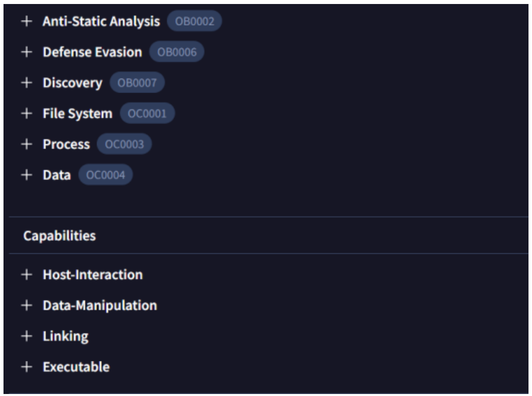
direct-cpu-clock-access long-sleeps persistence runtime-modules

MITRE ATT&CK Tactics and Techniques

+ Execution TA0002
+ Privilege Escalation TA0004
+ Defense Evasion TA0005
+ Discovery TA0007

Malware Behavior Catalog Tree

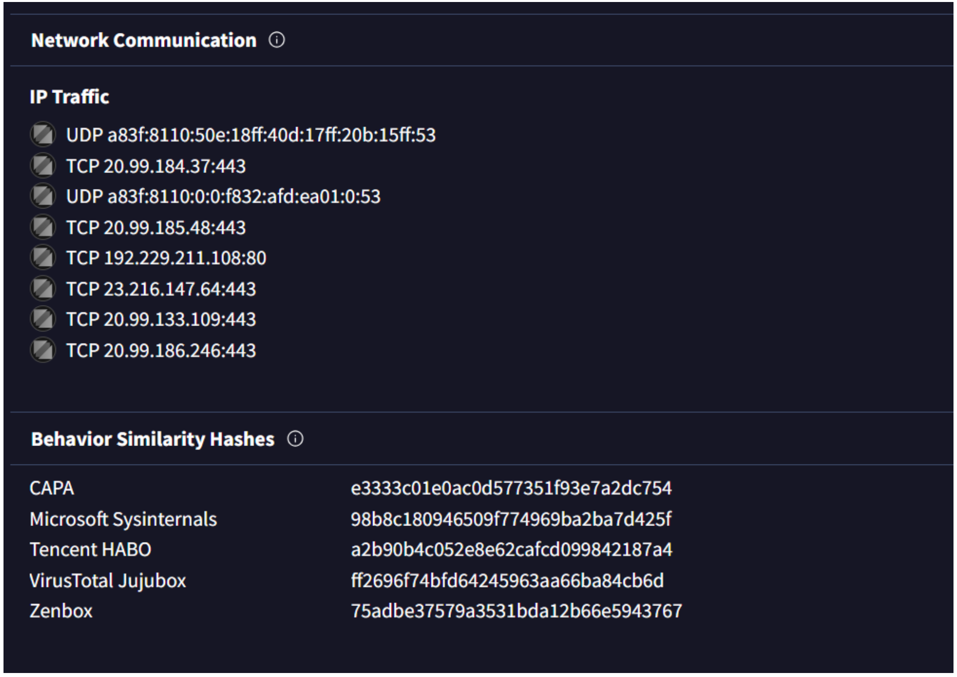
+ Anti-Behavioral Analysis OB0001
+ Anti-Static Analysis OB0002
+ Defense Evasion OB0006
+ Discovery OB0007
+ File System OC0001



- + Anti-Static Analysis OB0002
- + Defense Evasion OB0006
- + Discovery OB0007
- + File System OC0001
- + Process OC0003
- + Data OC0004

Capabilities

- + Host-Interaction
- + Data-Manipulation
- + Linking
- + Executable



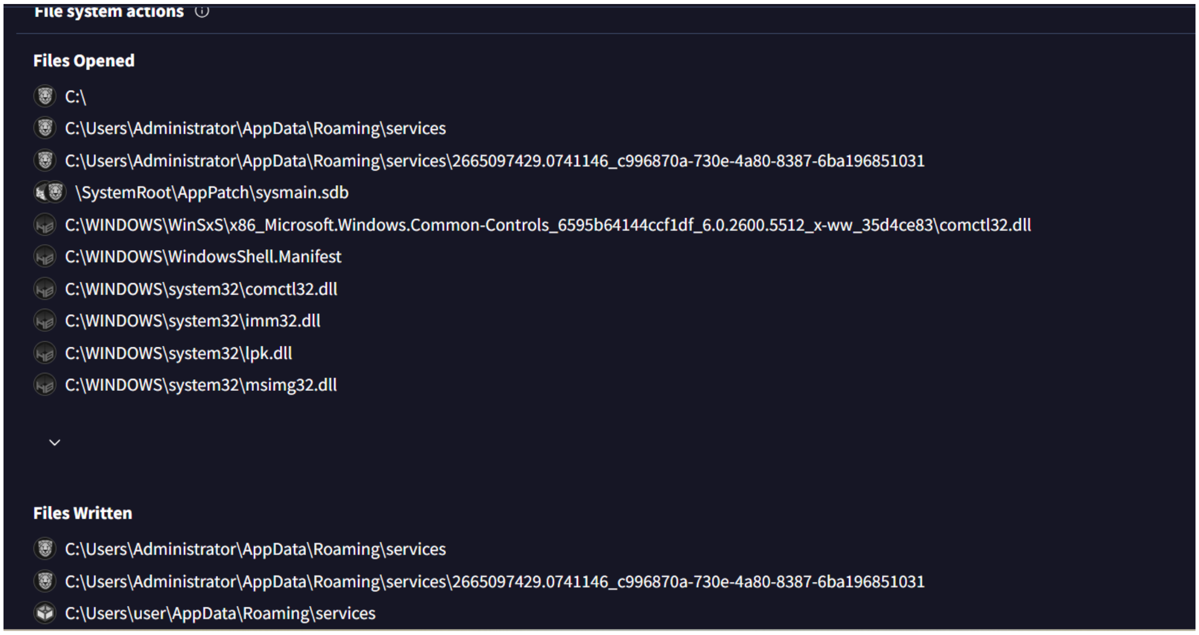
Network Communication ⓘ

IP Traffic

- UDP a83f:8110:50e:18ff:40d:17ff:20b:15ff:53
- TCP 20.99.184.37:443
- UDP a83f:8110:0:0:f832:afd:ea01:0:53
- TCP 20.99.185.48:443
- TCP 192.229.211.108:80
- TCP 23.216.147.64:443
- TCP 20.99.133.109:443
- TCP 20.99.186.246:443

Behavior Similarity Hashes ⓘ

CAPA	e3333c01e0ac0d577351f93e7a2dc754
Microsoft Sysinternals	98b8c180946509f774969ba2ba7d425f
Tencent HABO	a2b90b4c052e8e62cafcd099842187a4
VirusTotal Jujubox	ff2696f74bfd64245963aa66ba84cb6d
Zenbox	75adbe37579a3531bda12b66e5943767



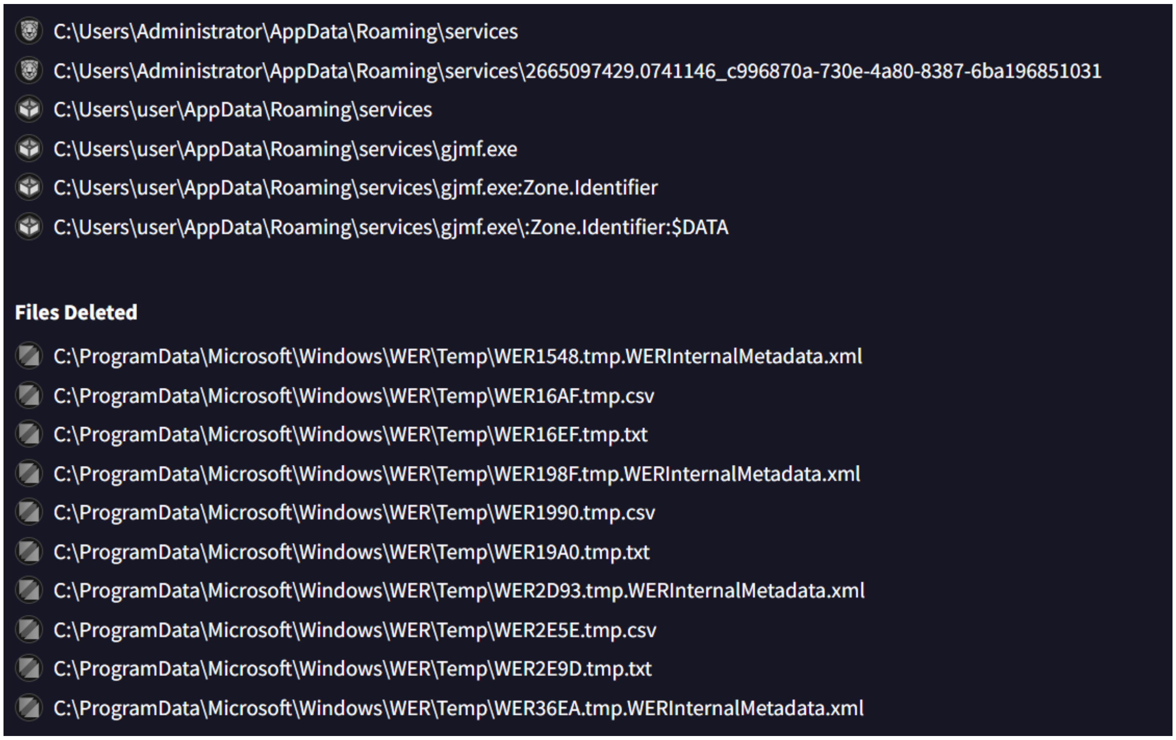
File system actions ⓘ

Files Opened

- C:\
- C:\Users\Administrator\AppData\Roaming\services
- C:\Users\Administrator\AppData\Roaming\services\2665097429.0741146_c996870a-730e-4a80-8387-6ba196851031
- \SystemRoot\AppPatch\sysmain.sdb
- C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
- C:\WINDOWS\WindowsShell.Manifest
- C:\WINDOWS\system32\comctl32.dll
- C:\WINDOWS\system32\imm32.dll
- C:\WINDOWS\system32\lpk.dll
- C:\WINDOWS\system32\msimg32.dll

Files Written

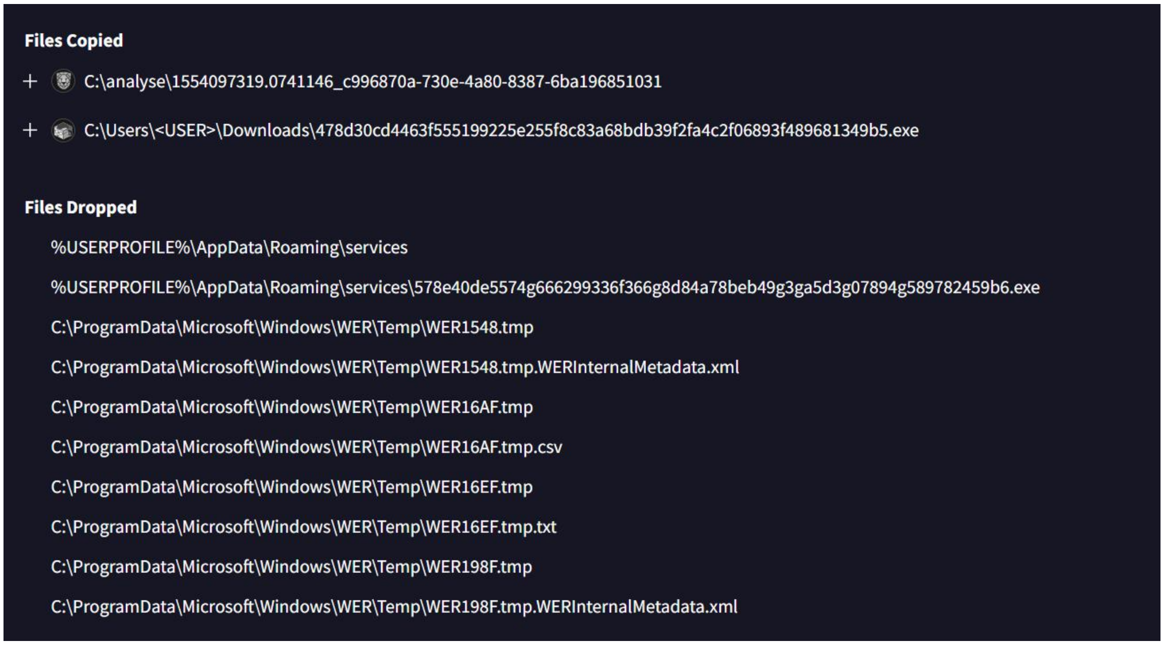
- C:\Users\Administrator\AppData\Roaming\services
- C:\Users\Administrator\AppData\Roaming\services\2665097429.0741146_c996870a-730e-4a80-8387-6ba196851031
- C:\Users\user\AppData\Roaming\services



```
C:\Users\Administrator\AppData\Roaming\services
C:\Users\Administrator\AppData\Roaming\services\2665097429.0741146_c996870a-730e-4a80-8387-6ba196851031
C:\Users\user\AppData\Roaming\services
C:\Users\user\AppData\Roaming\services\gjmf.exe
C:\Users\user\AppData\Roaming\services\gjmf.exe:Zone.Identifier
C:\Users\user\AppData\Roaming\services\gjmf.exe\:Zone.Identifier:$DATA
```

Files Deleted

```
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1548.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16AF.tmp.csv
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16EF.tmp.txt
C:\ProgramData\Microsoft\Windows\WER\Temp\WER198F.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1990.tmp.csv
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19A0.tmp.txt
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D93.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E5E.tmp.csv
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E9D.tmp.txt
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36EA.tmp.WERInternalMetadata.xml
```

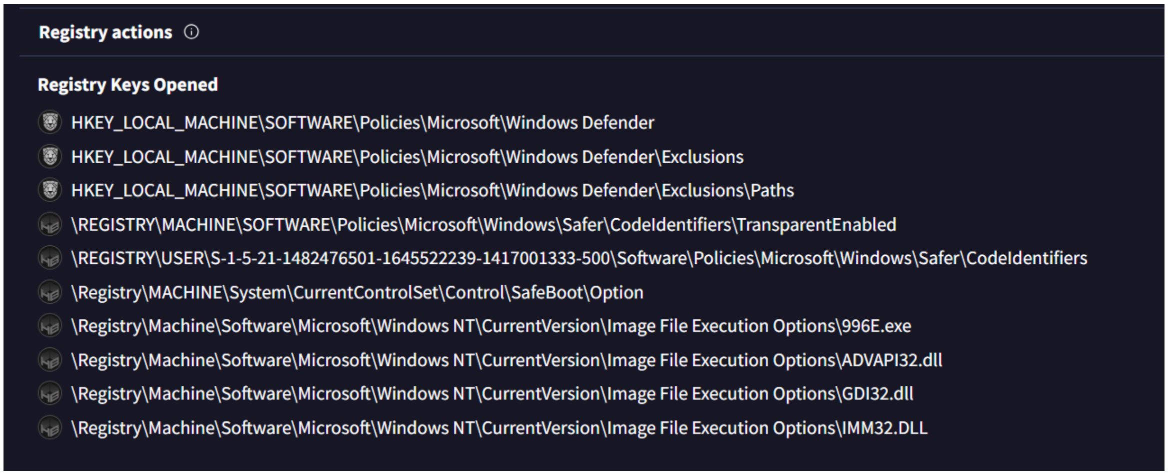


Files Copied

```
+ C:\analyse\1554097319.0741146_c996870a-730e-4a80-8387-6ba196851031
+ C:\Users\<USER>\Downloads\478d30cd4463f555199225e255f8c83a68bdb39f2fa4c2f06893f489681349b5.exe
```

Files Dropped

```
%USERPROFILE%\AppData\Roaming\services
%USERPROFILE%\AppData\Roaming\services\578e40de5574g666299336f366g8d84a78beb49g3ga5d3g07894g589782459b6.exe
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1548.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1548.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16AF.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16AF.tmp.csv
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16EF.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16EF.tmp.txt
C:\ProgramData\Microsoft\Windows\WER\Temp\WER198F.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WER198F.tmp.WERInternalMetadata.xml
```



Registry actions ⓘ

Registry Keys Opened

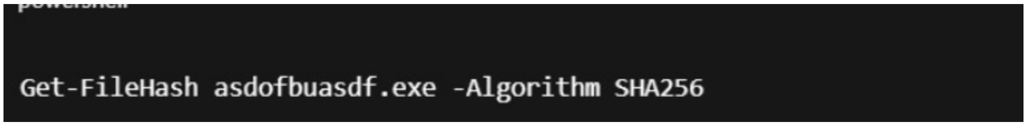
```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.exe
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADVAPI32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\GDI32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\IMM32.DLL
```

Static Analysis

Binary Analysis

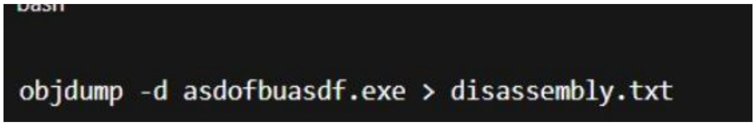
-Binary analysis involves studying the executable without running it.

-The malware is a PE32 file compiled for Windows, suspected to contain obfuscation and runtime-loaded modules.



```powershell
Get-FileHash asdofbuasdf.exe -Algorithm SHA256
```

Disassembly



```bash
objdump -d asdofbuasdf.exe > disassembly.txt
```

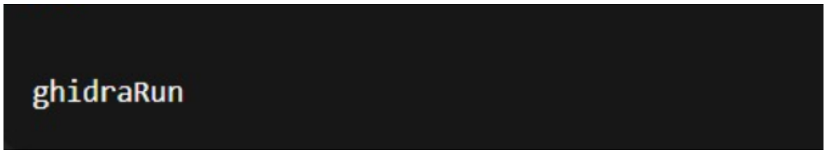
This command disassembles the file to human-readable assembly code.

Decompilation

-Tools like Ghidra or RetDec can reconstruct higher-level code for analysis.

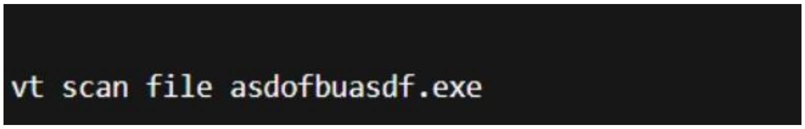
-Useful to detect logic such as spreading routines and payload downloaders.

Signature Analysis



```
ghidraRun
```

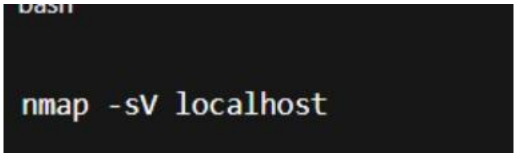
Check against malware databases:



```
vt scan file asdofbuasdf.exe
```

Dynamic Analysis

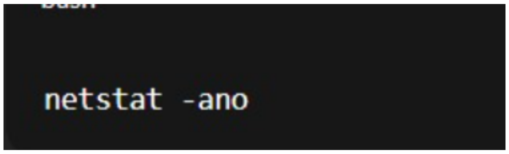
- Command 1: Nmap Scan for Open Ports



```bash
nmap -sV localhost
```

Detects open ports and running services.

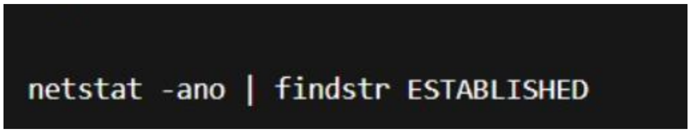
- Command 2: netstat -ano



```
netstat -ano
```

can reveal suspicious C2 connections.

-Command 3: Netstat with PID

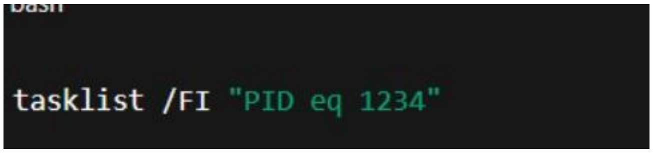


```
netstat -ano | findstr ESTABLISHED
```

Filters active established connections.

Associates suspicious connections with their PID.

- Command 4: Tasklist with PID

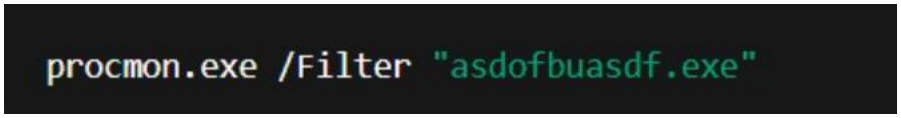


```
tasklist /FI "PID eq 1234"
```

Displays the process name tied to PID 1234.

Helps identify if malware injected into a legitimate process.

- Command 5: File Behavior Monitoring



```
procmon.exe /Filter "asdofbuasdf.exe"
```

Monitors registry edits, file writes, and persistence attempts.

What this PoC Intends to Achieve

-Static Analysis: Helps detect obfuscation, suspicious APIs, and embedded malicious logic.

-Dynamic Analysis: Uses Nmap, netstat, tasklist, and ProcMon to reveal live behavior like open ports, persistence, and spreading attempts.

-Outcome: Identifies W32.VBS_DufakaDGH.Trojan as a spreading Trojan with evasion techniques (sleep delays, CPU clock checks).

Proof-of-Concept (PoC) Objectives

1. Triggering core payload behavior (e.g., remote download, execution of commands, data exfiltration).

2. Demonstrating persistence or propagation mechanisms, if present (registry keys, dropped files).

3. Capturing observable artifacts:

    File paths, registry keys, network indicators (IPs, domains).

    Shell commands executed and processes spawned.

4. Safely demonstrating payload delivery and impact, without actually spreading or executing harmful actions in production.

5. Documenting the behavior clearly, including screenshots or logs—this becomes a reference for detection or mitigation.