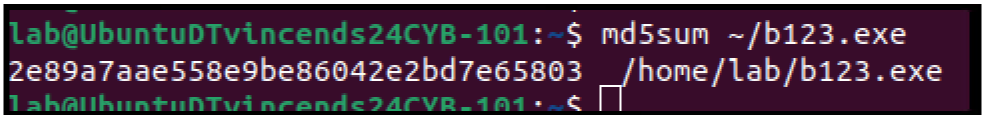
Definitions:

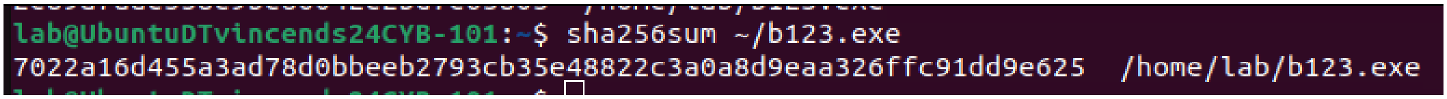
File hash: a strand of numbers you use to identify if the file has been changed or mutated since you last edited the file. It is also helpful to find the file on different websites.
MD5sum: This is important because you can use it to find a type of file hash. Then, you can use this file hash on websites like virustoatl.com to see if any other files with that same file hash have been reported as malicious.
SHA256Sum: SHA256 is more reliable because it produces a 256-bit hash value, Which decreases the probability of a file misread. This means you will have more accurate results when using this File hashing.
Mim type: This tells you what type of file it is. This is important because it tells your computer how to run the file. For example, if it is a PDF, it must open in a PDF file instead of a .dox file reader.
File Header: This label tells the computer the actual file type. It is essential because it will tell you if the name has been changed to a different file type, allowing you to detect destructive files.
Sand Box: A place where you can run known destructive files that will not hurt your machine and still be able to tell what it is doing.
Malware: This is any software intended to hurt someone's computer.

File Information:
File Name: b123.exe
MD5sum:



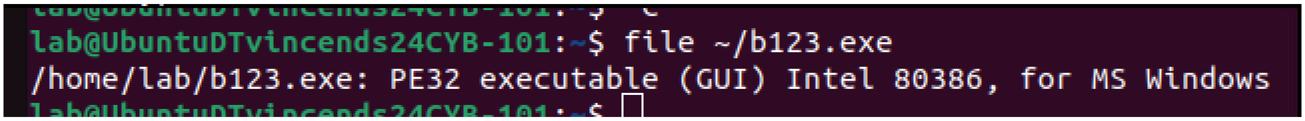
```
lab@UbuntuDTvincends24CYB-101:~$ md5sum ~/b123.exe
2e89a7aae558e9be86042e2bd7e65803  /home/lab/b123.exe
```

SHA256sum:



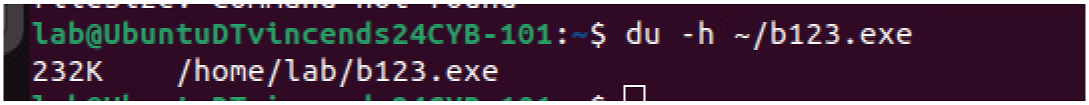
```
lab@UbuntuDTvincends24CYB-101:~$ sha256sum ~/b123.exe
7022a16d455a3ad78d0bbeeb2793cb35e48822c3a0a8d9eaa326ffc91dd9e625  /home/lab/b123.exe
```

File Mime:



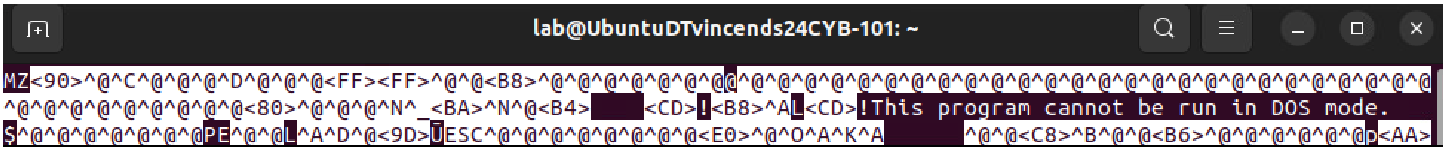
```
lab@UbuntuDTvincends24CYB-101:~$ file ~/b123.exe
/home/lab/b123.exe: PE32 executable (GUI) Intel 80386, for MS Windows
```

File Size:



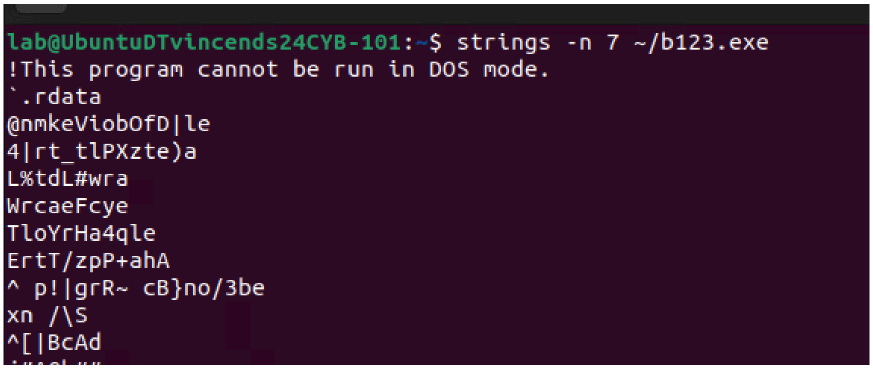
```
lab@UbuntuDTvincends24CYB-101:~$ du -h ~/b123.exe
232K    /home/lab/b123.exe
```

File Header:



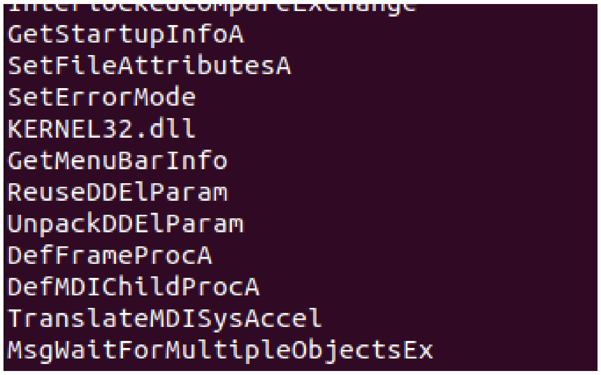
```
MZ<90>^@^C^@^@^@^D^@^@^@<FF><FF>^@^@<B8>^@^@^@^@^@^@^@@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@<80>^@^@^@^N^_<BA>^N^@<B4>     <CD>!<B8>^AL<CD>!This program cannot be run in DOS mode.
$^@^@^@^@^@^@^@PE^@^@L^A^D^@<9D>UESC^@^@^@^@^@^@^@^@<E0>^@^O^A^K^A        ^@^@<C8>^B^@^@<B6>^@^@^@^@^@^@p<AA>
```

Strings -n 7
A.

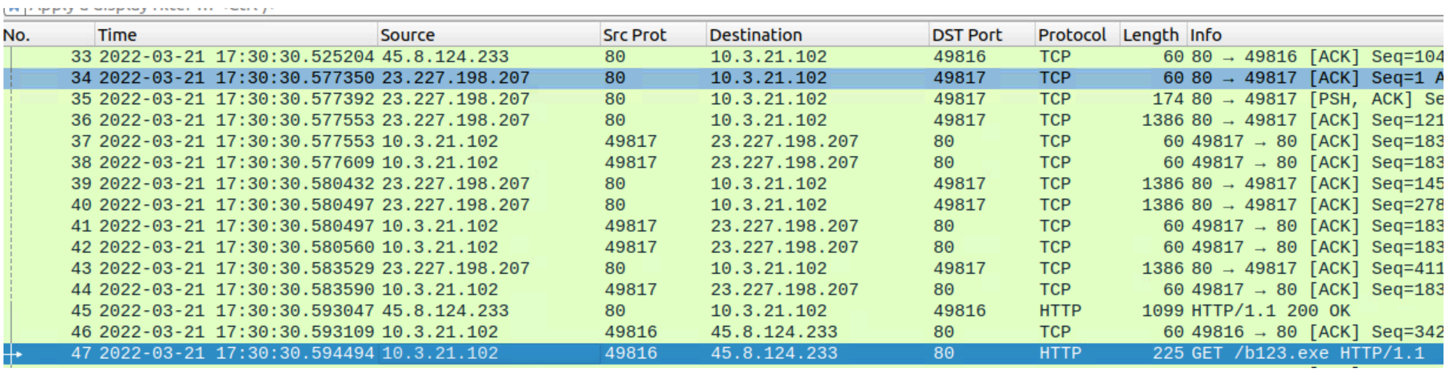


```
lab@UbuntuDTvincends24CYB-101:~$ strings -n 7 ~/b123.exe
!This program cannot be run in DOS mode.
`.rdata
@nmkeViobOfD|le
4|rt_tlPXzte)a
L%tdL#wra
WrcaeFcye
TloYrHa4qle
ErtT/zpP+ahA
^ p!|grR~ cB}no/3be
xn /\S
^[|BcAd
```

B.

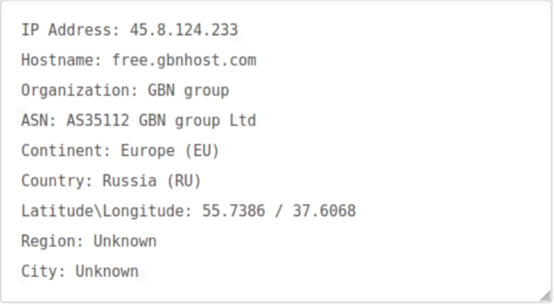


```
InterlockedCompareExchange
GetStartupInfoA
SetFileAttributesA
SetErrorMode
KERNEL32.dll
GetMenuBarInfo
ReuseDDElParam
UnpackDDElParam
DefFrameProcA
DefMDIChildProcA
TranslateMDISysAccel
MsgWaitForMultipleObjectsEx
```



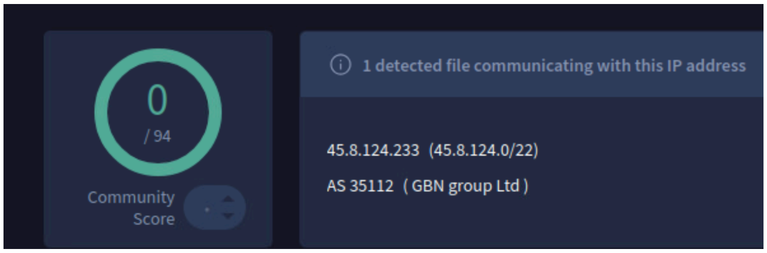
No.	Time	Source	Src Prot	Destination	DST Port	Protocol	Length	Info
33	2022-03-21 17:30:30.525204	45.8.124.233	80	10.3.21.102	49816	TCP	60	80 → 49816 [ACK] Seq=104
34	2022-03-21 17:30:30.577350	23.227.198.207	80	10.3.21.102	49817	TCP	60	80 → 49817 [ACK] Seq=1 A
35	2022-03-21 17:30:30.577392	23.227.198.207	80	10.3.21.102	49817	TCP	174	80 → 49817 [PSH, ACK] Se
36	2022-03-21 17:30:30.577553	23.227.198.207	80	10.3.21.102	49817	TCP	1386	80 → 49817 [ACK] Seq=121
37	2022-03-21 17:30:30.577553	10.3.21.102	49817	23.227.198.207	80	TCP	60	49817 → 80 [ACK] Seq=183
38	2022-03-21 17:30:30.577609	10.3.21.102	49817	23.227.198.207	80	TCP	60	49817 → 80 [ACK] Seq=183
39	2022-03-21 17:30:30.580432	23.227.198.207	80	10.3.21.102	49817	TCP	1386	80 → 49817 [ACK] Seq=145
40	2022-03-21 17:30:30.580497	23.227.198.207	80	10.3.21.102	49817	TCP	1386	80 → 49817 [ACK] Seq=278
41	2022-03-21 17:30:30.580497	10.3.21.102	49817	23.227.198.207	80	TCP	60	49817 → 80 [ACK] Seq=183
42	2022-03-21 17:30:30.580560	10.3.21.102	49817	23.227.198.207	80	TCP	60	49817 → 80 [ACK] Seq=183
43	2022-03-21 17:30:30.583529	23.227.198.207	80	10.3.21.102	49817	TCP	1386	80 → 49817 [ACK] Seq=411
44	2022-03-21 17:30:30.583590	10.3.21.102	49817	23.227.198.207	80	TCP	60	49817 → 80 [ACK] Seq=183
45	2022-03-21 17:30:30.593047	45.8.124.233	80	10.3.21.102	49816	HTTP	1099	HTTP/1.1 200 OK
46	2022-03-21 17:30:30.593109	10.3.21.102	49816	45.8.124.233	80	TCP	60	49816 → 80 [ACK] Seq=342
47	2022-03-21 17:30:30.594494	10.3.21.102	49816	45.8.124.233	80	HTTP	225	GET /b123.exe HTTP/1.1

IP Download from: 45.8.124.233
IP Download To: 10.3.21.102
UTC Time: 17:30:30.594494
IP Info:
IP Address:45.8.124.233
Geo Location: Russia
Country: Russia
Domain: @gbnhost.com



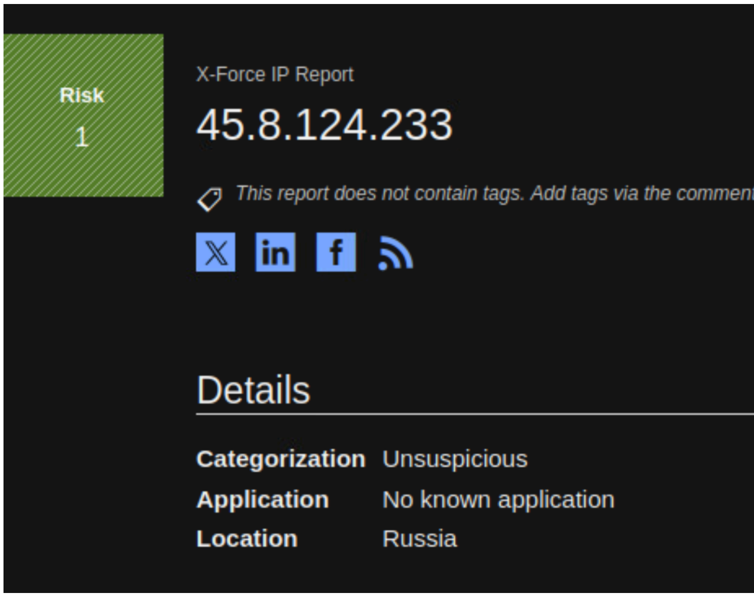
```
IP Address: 45.8.124.233
Hostname: free.gbnhost.com
Organization: GBN group
ASN: AS35112 GBN group Ltd
Continent: Europe (EU)
Country: Russia (RU)
Latitude\Longitude: 55.7386 / 37.6068
Region: Unknown
City: Unknown
```

Know Malicious: This IP address comes up with a 1 when you run it through IP Checkers. It is not known as malicious. Also, when you run it through Virustotal, 2/94 vendors flag it as malicious.



1 detected file communicating with this IP address

45.8.124.233 (45.8.124.0/22)
AS 35112 (GBN group Ltd)



X-Force IP Report

45.8.124.233

This report does not contain tags. Add tags via the comment

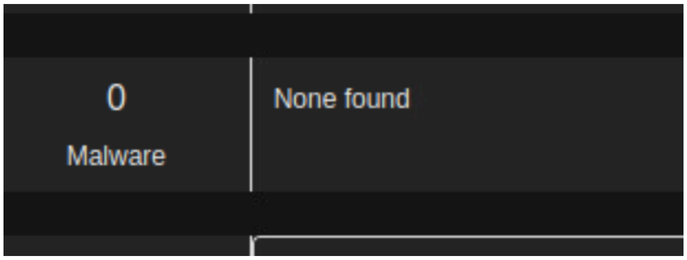
Details

Categorization	Unsuspicious
Application	No known application
Location	Russia

Domain Info:
Domain Name: @gbnhost.com
Domain IPs:

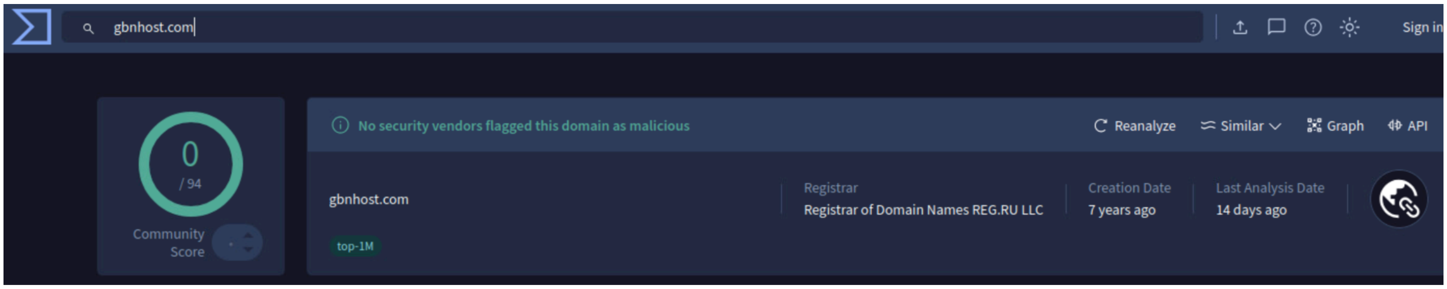
- 45.8.126.9,
- 45.8.8.126,
- 146.185.239
- 45.8.125.3,
- 45.8.126.16

Registered Info:REG.RU LLC
Malicious Domain?: With the information from Virus Total and X-Force Exchange giving the same conclusions, I caution you that it is a malicious domain. X-Force found six malicious files under this domain. Virus Total found 0 malicious files because of the community score of 0/94.



0
Malware

None found



gbnhost.com

0
/ 94
Community Score

No security vendors flagged this domain as malicious

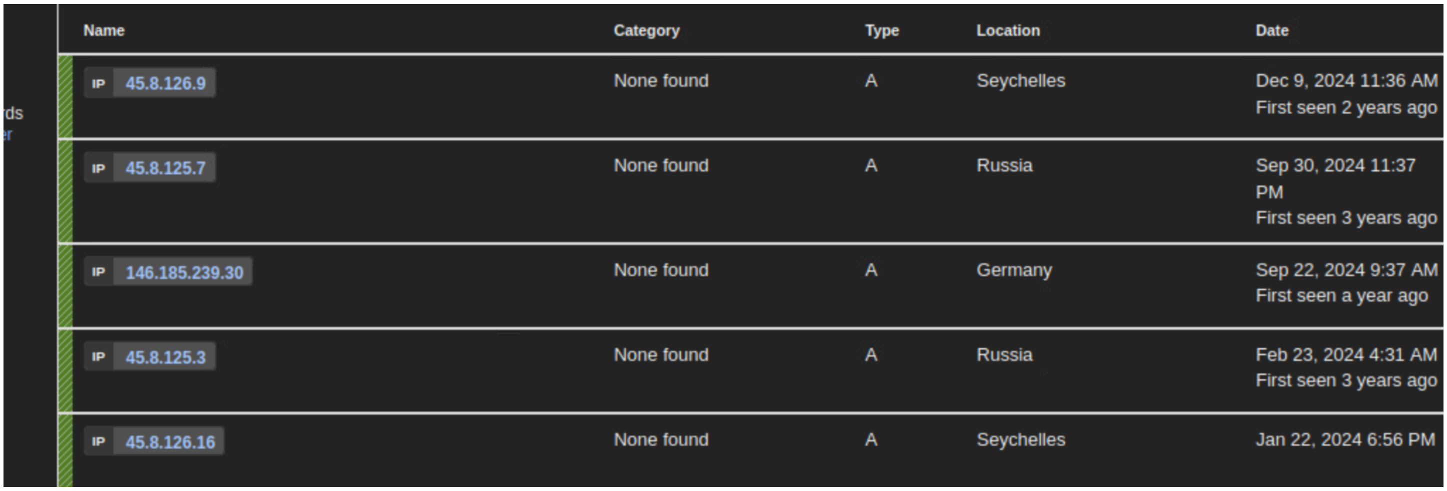
gbnhost.com

top-1M

Registrar
Registrar of Domain Names REG.RU LLC

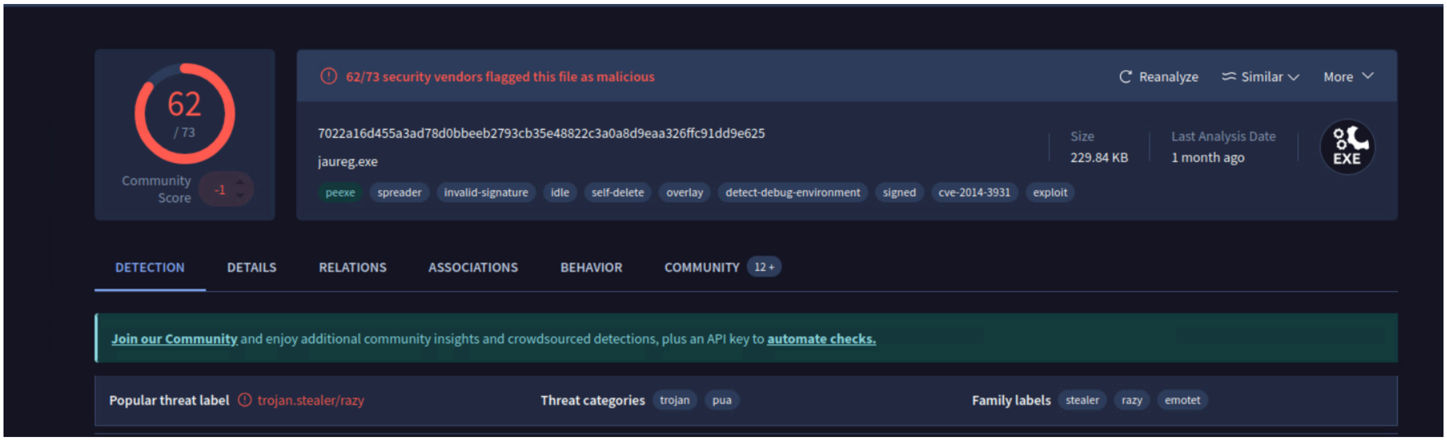
Creation Date
7 years ago

Last Analysis Date
14 days ago



Name	Category	Type	Location	Date
IP 45.8.126.9	None found	A	Seychelles	Dec 9, 2024 11:36 AM First seen 2 years ago
IP 45.8.125.7	None found	A	Russia	Sep 30, 2024 11:37 PM First seen 3 years ago
IP 146.185.239.30	None found	A	Germany	Sep 22, 2024 9:37 AM First seen a year ago
IP 45.8.125.3	None found	A	Russia	Feb 23, 2024 4:31 AM First seen 3 years ago
IP 45.8.126.16	None found	A	Seychelles	Jan 22, 2024 6:56 PM

The b123.exe file has been detected by 62 of 73 cybersecurity analyst vendors, determining that this file is very malicious. It has been diagnosed as a trojan, a file that hides in your system, giving the file's creator data remotely.



62
/ 73
Community Score -1

62/73 security vendors flagged this file as malicious

7022a16d455a3ad78d0bbeeb2793cb35e48822c3a0a8d9eaa326ffc91dd9e625
jaureg.exe

peexe spreader invalid-signature idle self-delete overlay detect-debug-environment signed cve-2014-3931 exploit

Size
229.84 KB

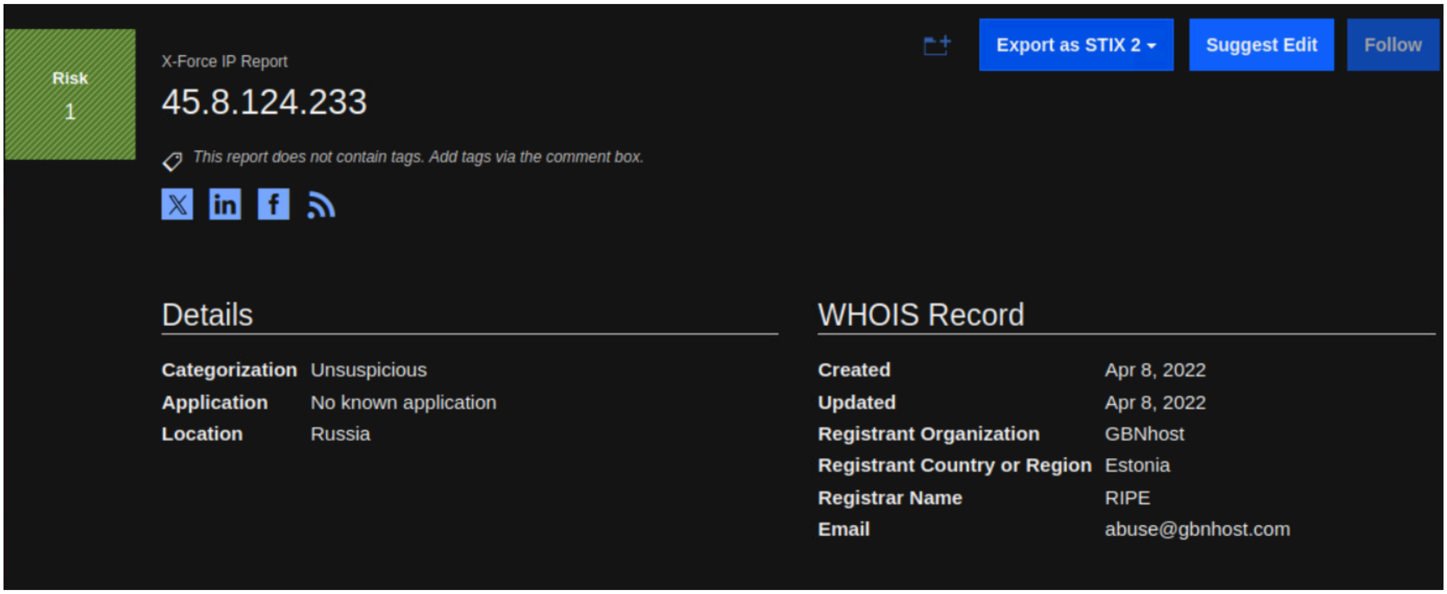
Last Analysis Date
1 month ago

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

Popular threat label trojan.stealer/razy

Threat categories trojan pua

Family labels stealer razy emotet



Risk
1

X-Force IP Report

45.8.124.233

This report does not contain tags. Add tags via the comment box.

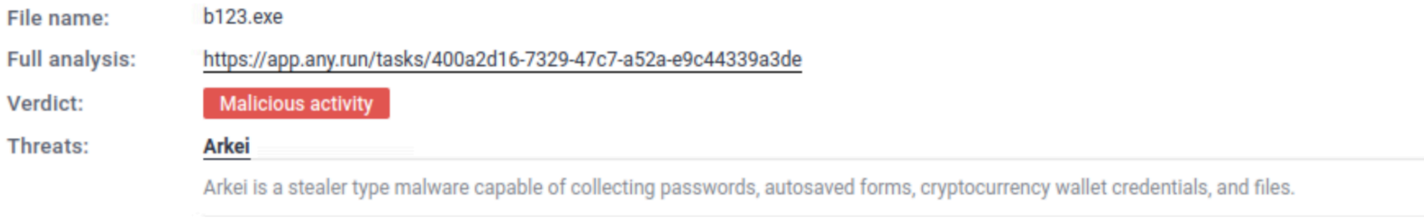
Details

Categorization	Unsuspicious
Application	No known application
Location	Russia

WHOIS Record

Created	Apr 8, 2022
Updated	Apr 8, 2022
Registrant Organization	GBNhost
Registrant Country or Region	Estonia
Registrar Name	RIPE
Email	abuse@gbnhost.com

SnadBox:



File name:	b123.exe
Full analysis:	https://app.any.run/tasks/400a2d16-7329-47c7-a52a-e9c44339a3de
Verdict:	Malicious activity
Threats:	**Arkei**

Arkei is a stealer type malware capable of collecting passwords, autosaved forms, cryptocurrency wallet credentials, and files.

This sandbox tells me that when it simulated b123.exe, it showed an Arkei Threat type. This Arkei is a type of threat capable of collecting Passwords and other auto-saved information.

File Name: B123.exe
MIME: Application/vnd.microsoft.portable-executable
MD5: 2E89A7AAE558E9BE86042E2BD7e65803
SHA 256: 7022A16D455A3AD78D0BBEEB2793CB35E48822C3A0A8D9EAA326FFC91DD9E625
Tags: Arkei
Geographic Location: Russia
Domain: @gbnhost.com
IP: 45.8.124.233

- What the malware is used for, its purpose(s):
  - The Arkie malware exploits personal data, explicitly targeting sensitive information stored in managed databases. Its primary goal is to harvest and manipulate this data to commit identity theft and other fraudulent activities. (https://nordvpn.com/cybersecurity/threat-center/arkei/)

- How the malware is distributed:
  - Arkie malware often infiltrates systems through phishing emails, deceptive ads, cracked software, and social engineering tactics that promise free access to premium software. It also utilizes a tool called Smokeloader, an advanced modular malware designed to establish an initial foothold in the target system. (https://any.run/malware-trends/arkei/)

- Actions it can perform on its target(s)
  - Arkie malware is capable of many malicious activities, including system monitoring, data exfiltration, remote access, cryptojacking, file corruption, and network disruption.

- If it can be removed, how?:
  - To remove Arkie malware, disconnect from the network, boot into Safe Mode, use reputable anti-malware software, manually inspect and remove suspicious files, reset browsers and applications, restore the system from a clean backup, update the system and software, and implement measures to prevent future infections.

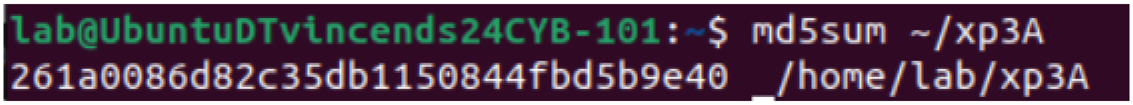
- How can it be detected?:
  - Arkie malware can be detected by monitoring unusual system activity, performing file hash matching, detecting Smokeloader, using file integrity monitoring, checking for suspicious connections, conducting port scanning, and utilizing deep scan tools.

- Any threat groups are known as the primary users/distributors of the malware:
  - Arkie malware is associated with cybercriminal groups like FIN7, Lazarus Group, and Carbanak Group, but there are no widely reported threat groups known explicitly as the primary users or distributors of the malware

- In both reports, provide how the malware persists on its target(s)with an explanation of the persistence mechanism(s).:
  - Arkie malware uses persistence mechanisms such as modifying the Windows registry to ensure it runs at startup and creating scheduled tasks that automatically execute the malware at specified intervals or when certain conditions are met.

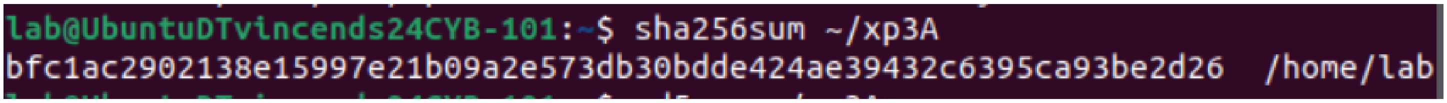
File Info
File Name: xp3A

Md5sum:



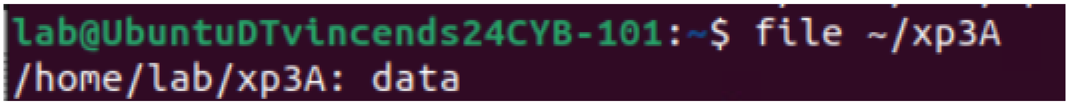
```
lab@UbuntuDTvincends24CYB-101:~$ md5sum ~/xp3A
261a0086d82c35db1150844fbd5b9e40  /home/lab/xp3A
```

Sha256:



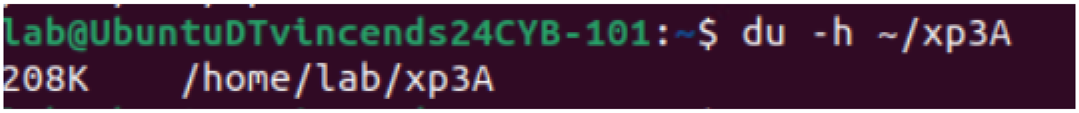
```
lab@UbuntuDTvincends24CYB-101:~$ sha256sum ~/xp3A
bfc1ac2902138e15997e21b09a2e573db30bdde424ae39432c6395ca93be2d26  /home/lab
```

File Mime:



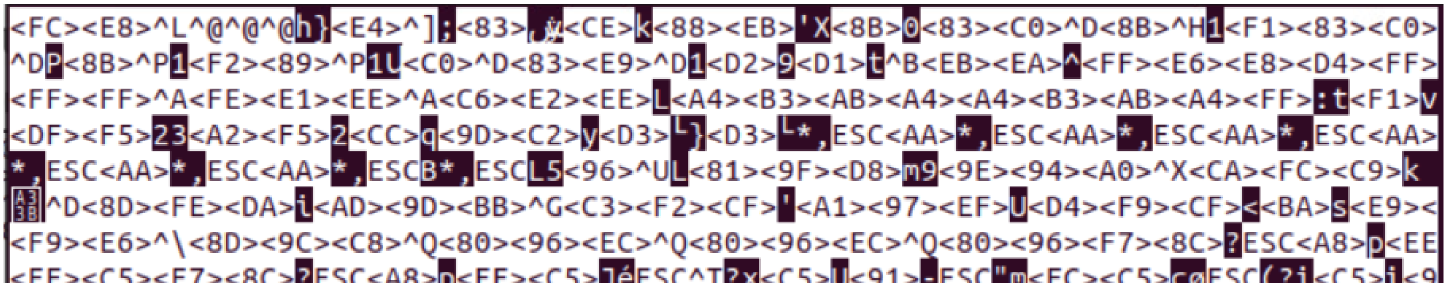
```
lab@UbuntuDTvincends24CYB-101:~$ file ~/xp3A
/home/lab/xp3A: data
```

File Size



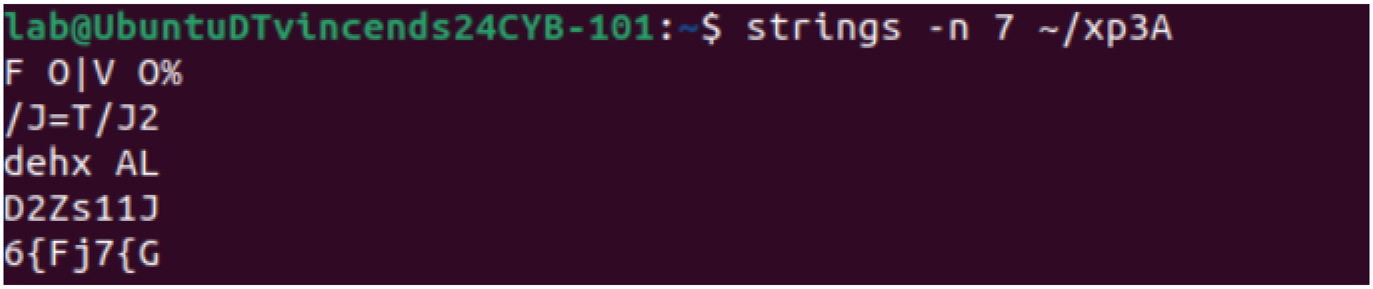
```
lab@UbuntuDTvincends24CYB-101:~$ du -h ~/xp3A
208K    /home/lab/xp3A
```

File Header

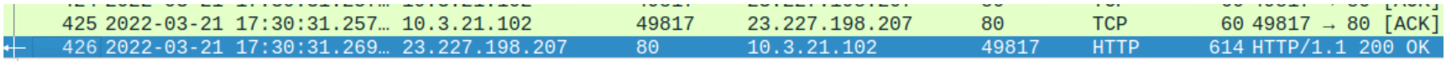


```
<FC><E8>^L^@^@^@h}<E4>^];<83>,ÿ<CE>k<88><EB>'X<8B>0<83><C0>^D<8B>^H1<F1><83><C0>
^DP<8B>^P1<F2><89>^P1l<C0>^D<83><E9>^D1<D2>9<D1>t^B<EB><EA>^<FF><E6><E8><D4><FF>
<FF><FF>^A<FE><E1><EE>^A<C6><E2><EE>L<A4><B3><AB><A4><A4><B3><AB><A4><FF>:t<F1>v
<DF><F5>23<A2><F5>2<CC>q<9D><C2>y<D3>└}<D3>└*,ESC<AA>*,ESC<AA>*,ESC<AA>*,ESC<AA>
*,ESC<AA>*,ESC<AA>*,ESCB*,ESCL5<96>^UL<81><9F><D8>m9<9E><94><A0>^X<CA><FC><C9>k
ꌻ^D<8D><FE><DA>i<AD><9D><BB>^G<C3><F2><CF>'<A1><97><EF>U<D4><F9><CF><<BA>s<E9><
<F9><E6>^\<8D><9C><C8>^Q<80><96><EC>^Q<80><96><EC>^Q<80><96><F7><8C>?ESC<A8>p<EE
<FF><C5><F7><8C>?ESC<A8>p<FF><C5>JéESC^T?x<C5>U<91>-ESC"m<FC><C5>cøESC(?i<C5>i<9
```

String -n 7

A. 

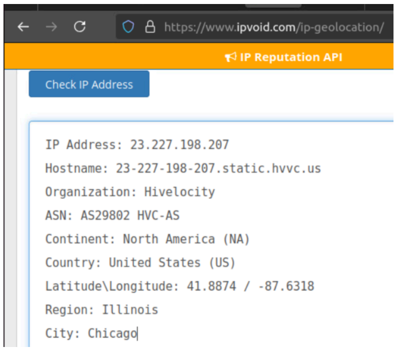
```
lab@UbuntuDTvincends24CYB-101:~$ strings -n 7 ~/xp3A
F O|V O%
/J=T/J2
dehx AL
D2Zs11J
6{Fj7{G
```



```
425 2022-03-21 17:30:31.257… 10.3.21.102     49817  23.227.198.207  80     TCP   60 49817 → 80 [ACK]
426 2022-03-21 17:30:31.269… 23.227.198.207  80     10.3.21.102     49817  HTTP  614 HTTP/1.1 200 OK
```

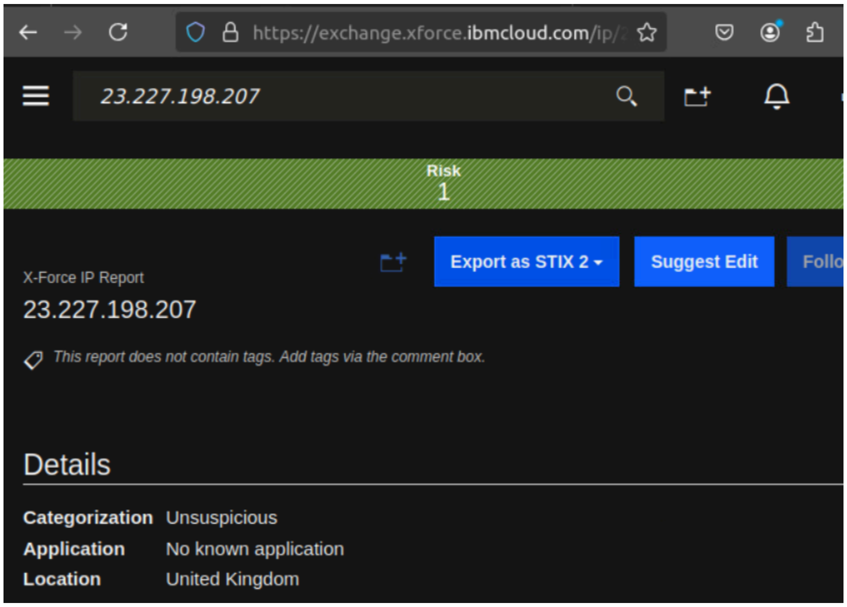
IP Download from: 23.227.198.207
IP Download To: 10.3.21.102
UTC Time: 17:30:30.433

IP Info:
IP Address: 23.227.198.207
Geo Location: Chicago, Illinois
Country: United States
Domain: @hivelocity.net



IP Address: 23.227.198.207
Hostname: 23-227-198-207.static.hvvc.us
Organization: Hivelocity
ASN: AS29802 HVC-AS
Continent: North America (NA)
Country: United States (US)
Latitude\Longitude: 41.8874 / -87.6318
Region: Illinois
City: Chicago

Know Malicious: This IP address comes up with a 1 when you run it through IP Checkers. It is not known as malicious. Also, when you run it through Virustotal, 2/94 vendors flag it as malicious.



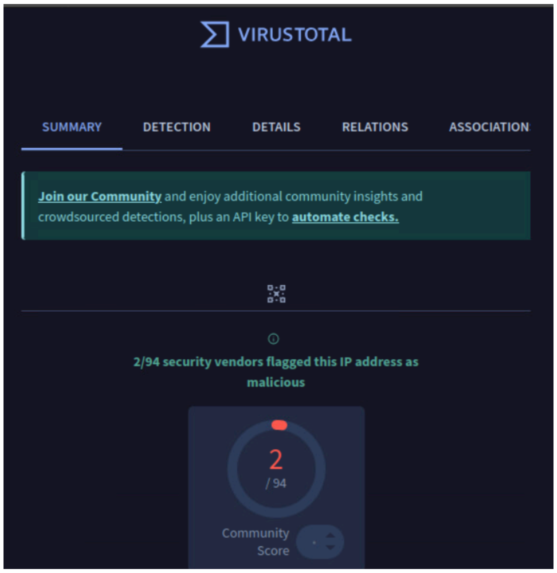
X-Force IP Report

23.227.198.207

This report does not contain tags. Add tags via the comment box.

Details

Categorization	Unsuspicious
Application	No known application
Location	United Kingdom

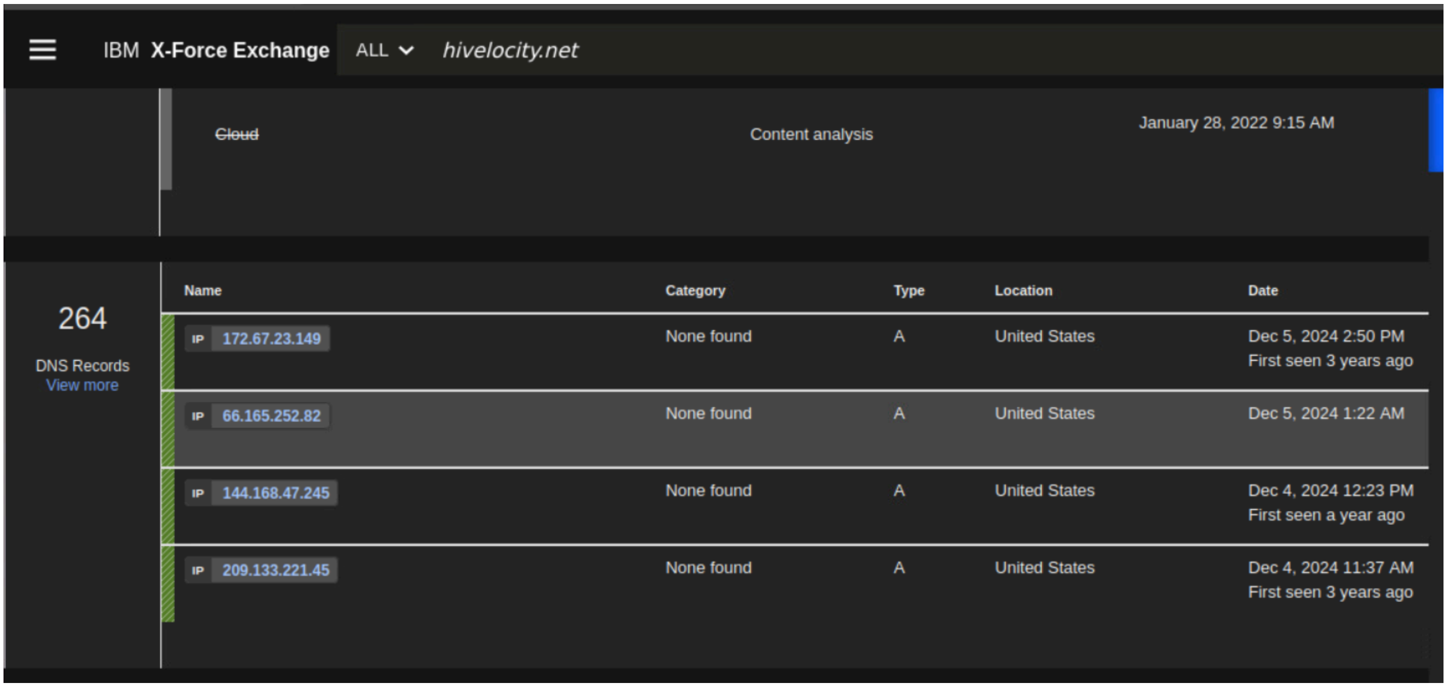


Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

2/94 security vendors flagged this IP address as malicious

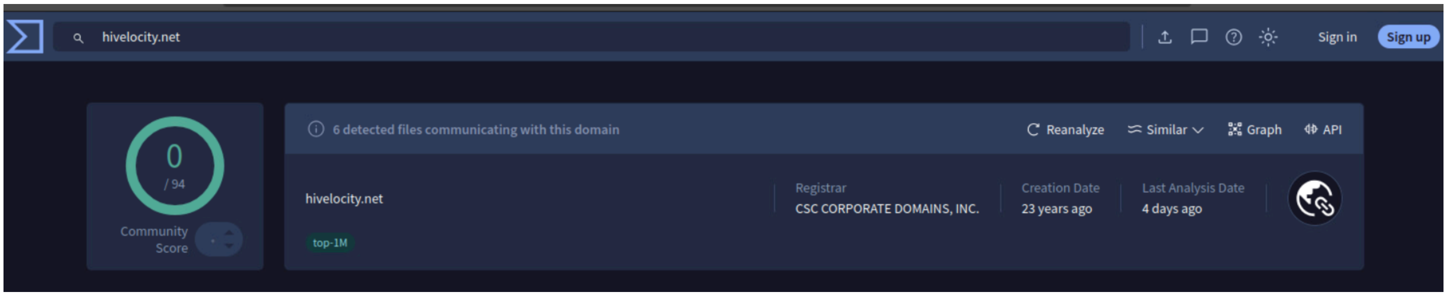
Domain Info:
Domain Name: @hivelocity.net
Domain IPs:

- 172.67.23.149
- 66.165.252.82
- 144.168.47.254
- 209.133.221.45



Name	Category	Type	Location	Date
IP 172.67.23.149	None found	A	United States	Dec 5, 2024 2:50 PM First seen 3 years ago
IP 66.165.252.82	None found	A	United States	Dec 5, 2024 1:22 AM
IP 144.168.47.245	None found	A	United States	Dec 4, 2024 12:23 PM First seen a year ago
IP 209.133.221.45	None found	A	United States	Dec 4, 2024 11:37 AM First seen 3 years ago

Regisars Information: Csc Corporation Domains, INC.
Malicious Domain?: With the information from Virus Total and X-Force Exchange giving different conclusions, I caution you that it is a malicious domain. X-Force found six malicious files under this domain. Virus Total found 0 malicious files because of the community score of 0/94.



hivelocity.net

Sign in | Sign up

0 / 94 Community Score

6 detected files communicating with this domain

Reanalyze | Similar | Graph | API

hivelocity.net

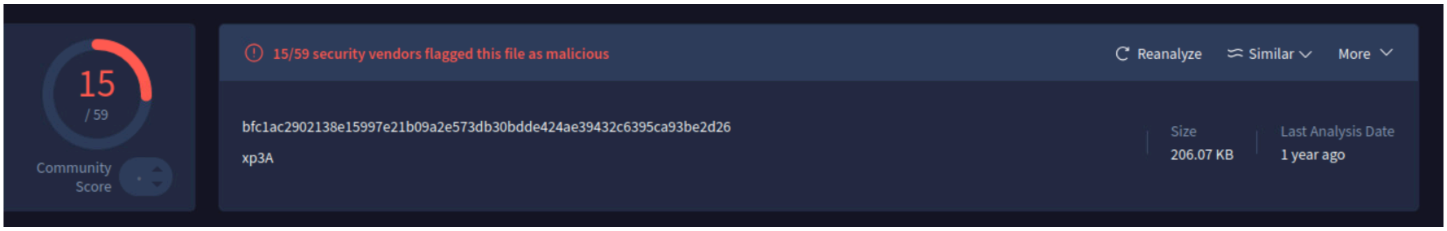
top-1M

Registrar: CSC CORPORATE DOMAINS, INC.

Creation Date: 23 years ago

Last Analysis Date: 4 days ago

File Findings:



15 / 59 Community Score

15/59 security vendors flagged this file as malicious

Reanalyze | Similar | More

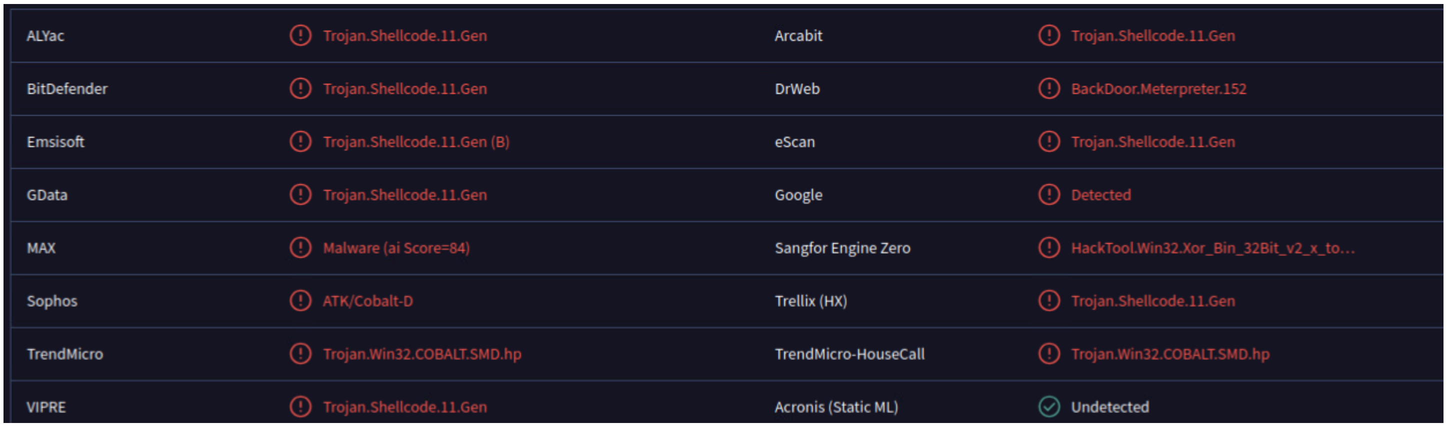
bfc1ac2902138e15997e21b09a2e573db30bdde424ae39432c6395ca93be2d26

xp3A

Size: 206.07 KB

Last Analysis Date: 1 year ago

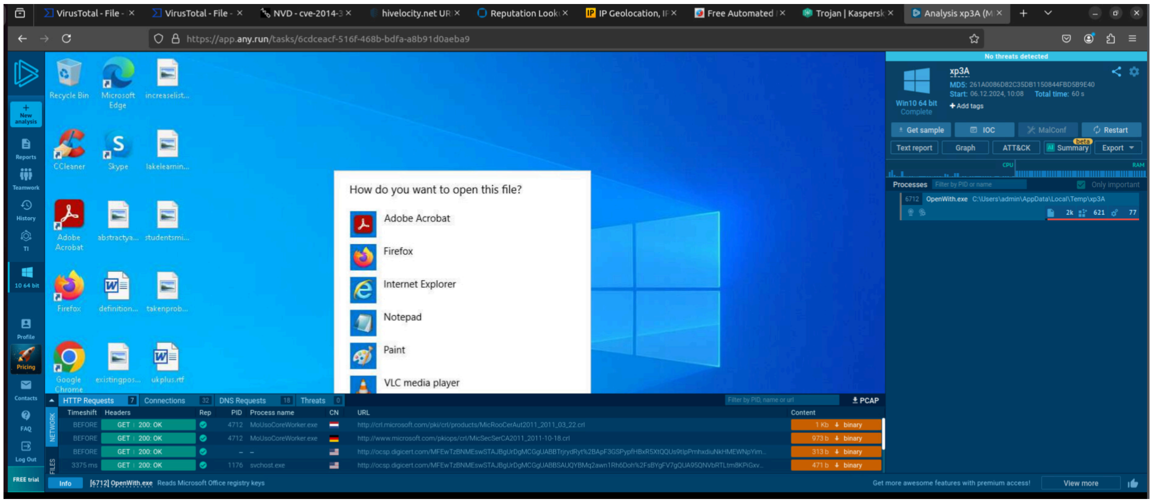
Malicious? This file has a community score of 15/59, which means that 15 vendors reported that they had detected it to be malicious. This file is malicious because, when investigated, it looks like it has enough data to validate it.



ALYac	Trojan.Shellcode.11.Gen	Arcabit	Trojan.Shellcode.11.Gen
BitDefender	Trojan.Shellcode.11.Gen	DrWeb	BackDoor.Meterpreter.152
Emsisoft	Trojan.Shellcode.11.Gen (B)	eScan	Trojan.Shellcode.11.Gen
GData	Trojan.Shellcode.11.Gen	Google	Detected
MAX	Malware (ai Score=84)	Sangfor Engine Zero	HackTool.Win32.Xor_Bin_32Bit_v2_x_to...
Sophos	ATK/Cobalt-D	Trellix (HX)	Trojan.Shellcode.11.Gen
TrendMicro	Trojan.Win32.COBALT.SMD.hp	TrendMicro-HouseCall	Trojan.Win32.COBALT.SMD.hp
VIPRE	Trojan.Shellcode.11.Gen	Acronis (Static ML)	✓ Undetected

Type of Malware: The malware that was detected the most was Trojan.Shellcode. This Malware is known for spying on people's computers. They can block and restrict security measures people have put on their machines. This also can send data that you were researching back to the owner.

Sandbox:



https://app.any.run/tasks/6cdceacf-516f-468b-bdfa-a8b91d0aeba9

How do you want to open this file?

- Adobe Acrobat
- Firefox
- Internet Explorer
- Notepad
- Paint
- VLC media player

No threats detected

xp3A

MD5: 261A0086D82C35DB1150844FBD5B9E40

Start: 06.12.2024, 10:08 Total time: 60 s

Win10 64 bit Complete

Get sample | IOC | MalConf | Restart

Text report | Graph | ATT&CK | Summary | Export

Processes

6712 OpenWith.exe C:\Users\admin\AppData\Local\Temp\xp3A 2k 621 77

HTTP Requests 7 | Connections 32 | DNS Requests 18 | Threats 0

```
Timeshift  Headers        Rep  PID   Process name         CN  URL                                                                                          Content
BEFORE     GET  200: OK         4712  MoUsoCoreWorker.exe      http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl                    1 Kb  binary
BEFORE     GET  200: OK         4712  MoUsoCoreWorker.exe      http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl                           973 b  binary
BEFORE     GET  200: OK         –     –                        http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tIpPmhxdiuNkHMEWNpYim...  313 b  binary
3375 ms    GET  200: OK         1176  svchost.exe              http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxv...  471 b  binary
```

Info [6712] OpenWith.exe Reads Microsoft Office registry keys

Get more awesome features with premium access! View more

This sandbox did not detect any malicious activity when executing this file.

File Name: xp3A
MIME: Data
MD5: 261a0086d82c35db1150844fbd5b9e40
SHA 256: 261a0086d82c35db1150844fbd5b9e40
Tags: trojan.shellcode/cobalt
Geographic Location: Chicago, Illinois
Country: United States
Domain: hivelocity.net
IP: 23.227.198.207

- What the malware is used for, its purpose(s):
  - Trojan.shellcode/cobalt is a malicious code commonly associated with the Cobalt Strike tool, a legitimate software suite originally designed for penetration testing but frequently repurposed by cybercriminals and threat actors for malicious activities.

- How the malware is distributed:
  - Trojan.shellcode/cobalt is commonly distributed through various attack methods, including phishing emails that trick users into opening malicious attachments or clicking infected links and exploit kits that target unpatched vulnerabilities in software or browsers. It can also spread via malicious advertisements (malvertising), which deliver malware when users click on seemingly legitimate ads, and through cracked or pirated software that contains hidden malicious code.

- Actions it can perform on its target(s)
  - Trojan.shellcode/cobalt is a versatile malware capable of performing various harmful actions on its targets. It establishes initial access and persistence by connecting to Command-and-Control (C2) servers and employing techniques like registry modifications or fileless operations to remain active. Once inside, it facilitates data exfiltration by stealing sensitive information such as credentials or financial data. It can also move laterally within networks, using exploits or stolen credentials to compromise additional systems. Through remote execution, the malware runs attacker-supplied commands or deploys further payloads like ransomware.

- If it can be removed, how?:
  - To remove Trojan.shellcode/cobal malware, disconnect from the network, boot into Safe Mode, use reputable anti-malware software, manually inspect and remove suspicious files, reset browsers and applications, restore the system from a clean backup, update the system and software, and implement measures to prevent future infections.

- How can it be detected?:
  - rojan.shellcode/cobalt can be detected through various methods that identify unusual behavior and malicious activities. Indicators include unusual system activity, such as unexpected slowdowns, unexplained file modifications, or strange processes running in the background

- Any threat groups are known as the primary users/distributors of the malware:
  - Trojan.shellcode/cobalt is primarily distributed and utilized by advanced threat groups, including FIN7, Lazarus Group, and Carbanak Group, although no widely reported group has been definitively identified as the sole distributor. These groups are known for sophisticated cyberattacks, often leveraging tools like Cobalt Strike for financial theft, espionage, or large-scale data breaches.

- Provide, in both reports, how the malware persists on its target(s)with an explanation of the persistence mechanism(s).:
    - Trojan.shellcode/cobalt uses several persistence mechanisms to remain on its target system, even after restarts or removal attempts. One key method is modifying the Windows registry, where it alters startup entries to ensure the malware is executed every time the system boots up