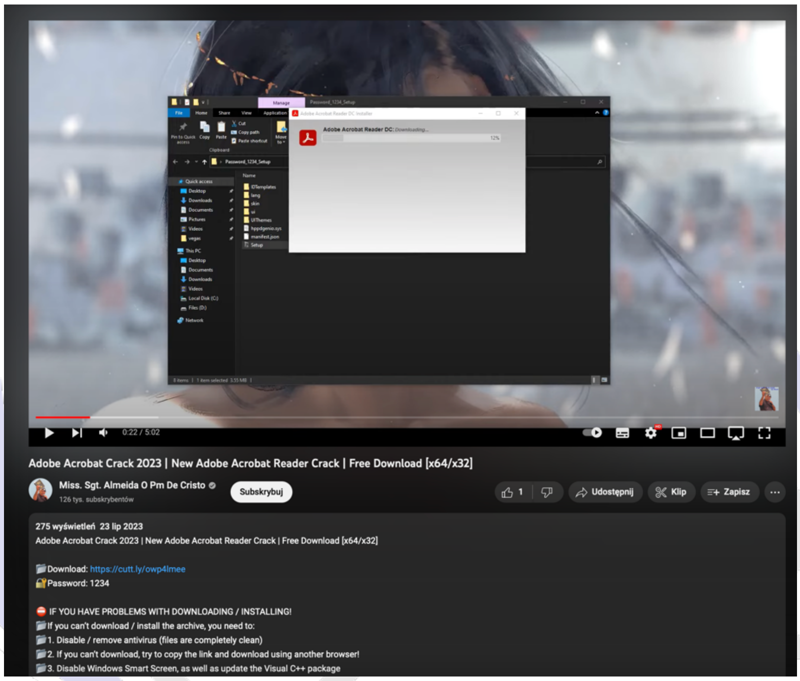
YouTube malware analysis

Analysis description:

This report is an analysis of malware found on the YouTube platform. It focuses on a specific case in which a download link from the description of a video was used, advertising crack software for the popular Acrobat Reader application. After downloading and analyzing the contents of the .rar file, it was found to contain malware focused on stealing information from the victim's device.



Adobe Acrobat Crack 2023 | New Adobe Acrobat Reader Crack | Free Download [x64/x32]

Miss. Sgt. Almeida O Pm De Cristo
126 tys. subskrybentów

275 wyświetleń 23 lip 2023
Adobe Acrobat Crack 2023 | New Adobe Acrobat Reader Crack | Free Download [x64/x32]

📁Download: https://cutt.ly/owp4lmee
🔐Password: 1234

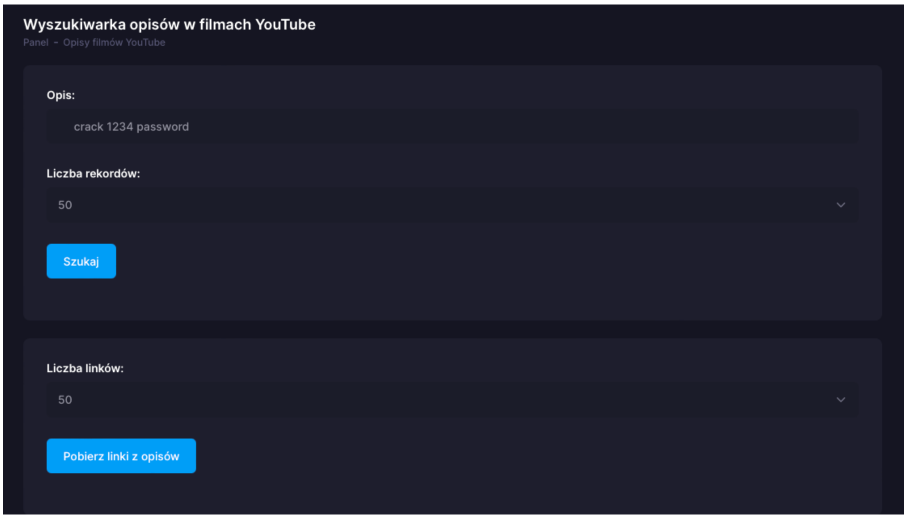
⛔ IF YOU HAVE PROBLEMS WITH DOWNLOADING / INSTALLING!
📁If you can't download / install the archive, you need to:
📁1. Disable / remove antivirus (files are completely clean)
📁2. If you can't download, try to copy the link and download using another browser!
📁3. Disable Windows Smart Screen, as well as update the Visual C++ package

The report also includes information about the localized IP addresses to which the malware was connecting. Subsequent .exe files that were downloaded and contacted the same IP addresses are analyzed. The analyses showed the presence of the same types of malware, with a few additional types discovered during the investigation.

The report highlights that all the malicious files examined communicated with two common IP addresses. In addition, using ETag analysis, it was possible to locate further IP addresses that could be used for the same purpose.

The document describes the process of identifying and analyzing the malware, demonstrating the steps that were taken to identify and understand the operation of the malware, as well as its communication points in the form of IP addresses.

1) **Searching for malware on the Youtube platform under the key phrase:** "password 1234 crack":



Wyszukiwarka opisów w filmach YouTube

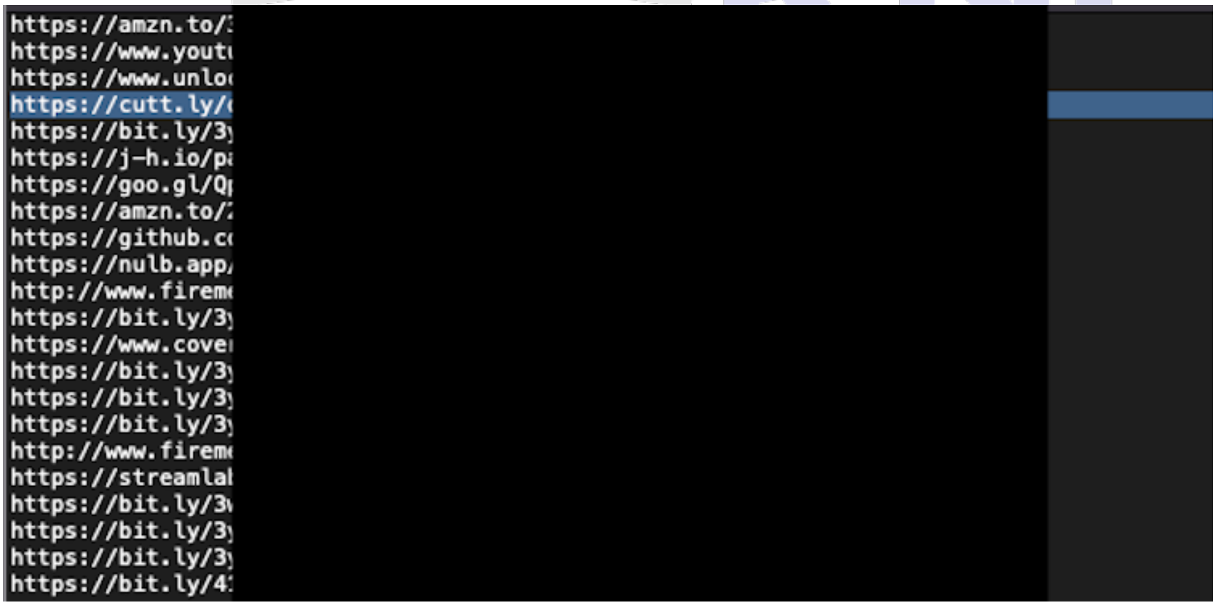
Panel - Opisy filmów YouTube

Opis: crack 1234 password

Liczba rekordów: 50

Liczba linków: 50

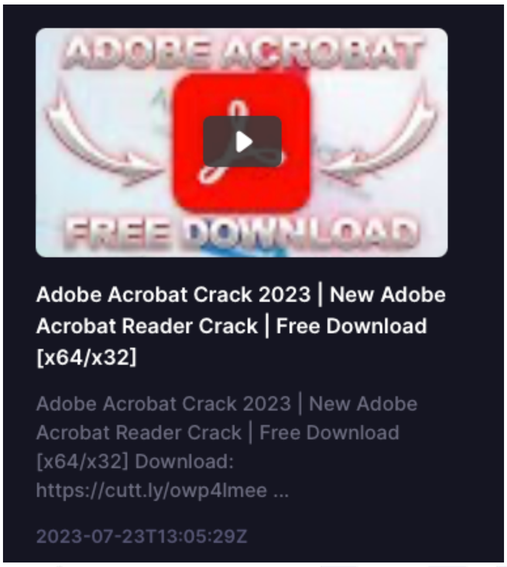
2) **Downloading links from descriptions and selecting one for analysis:**



```
https://amzn.to/
https://www.yout
https://www.unlo
https://cutt.ly/
https://bit.ly/3
https://j-h.io/p
https://goo.gl/Q
https://amzn.to/
https://github.c
https://nulb.app
http://www.firem
https://bit.ly/3
https://www.cove
https://bit.ly/3
https://bit.ly/3
https://bit.ly/3
http://www.firem
https://streamla
https://bit.ly/3
https://bit.ly/3
https://bit.ly/3
https://bit.ly/4
```

[redacted]

3) **Link to download crack software for popular application: Acrobat Reader** (Youtube video published on 23.07.2023):

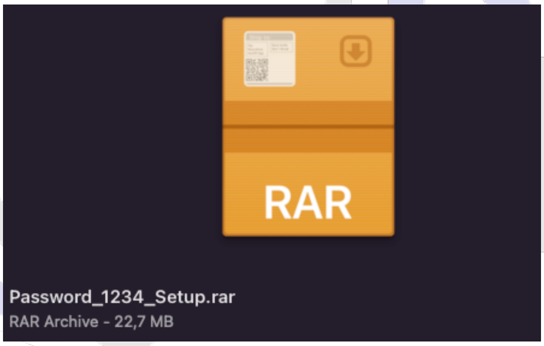


Adobe Acrobat Crack 2023 | New Adobe Acrobat Reader Crack | Free Download [x64/x32]

Adobe Acrobat Crack 2023 | New Adobe Acrobat Reader Crack | Free Download [x64/x32] Download: https://cutt.ly/owp4lmee ...

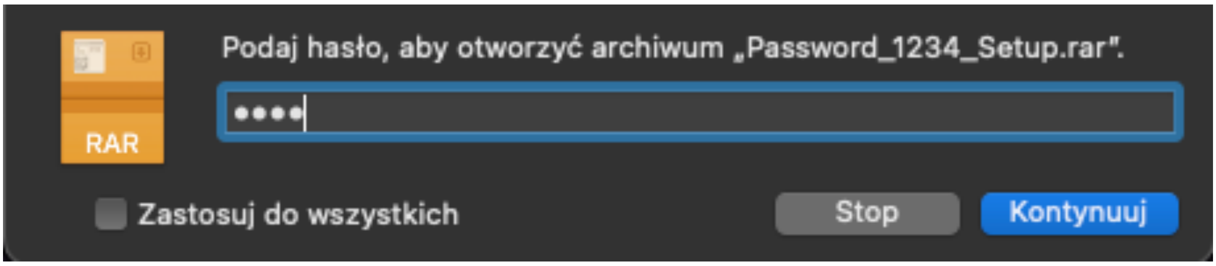
2023-07-23T13:05:29Z

4) **Download the .rar file from the link from the video description:**



Password_1234_Setup.rar
RAR Archive - 22,7 MB

5) **Entering the password from the description of the video into the archive and unpacking the contents:**

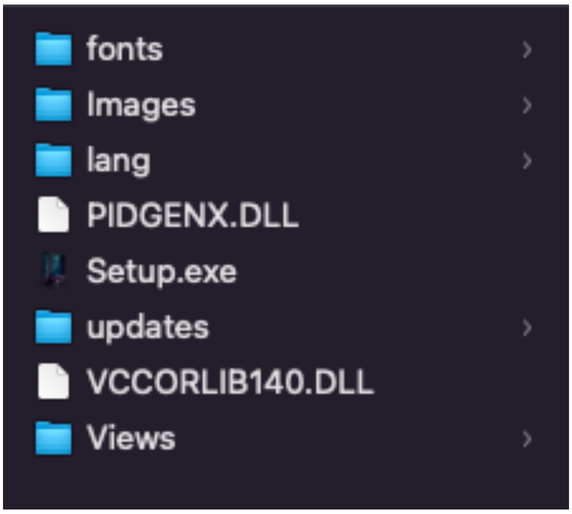


Podaj hasło, aby otworzyć archiwum „Password_1234_Setup.rar".

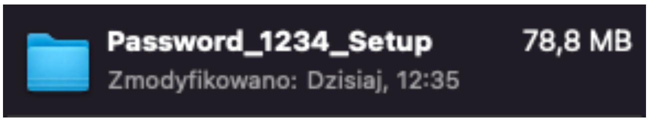
••••

□ Zastosuj do wszystkich

6) **Contents of .rar archive. Size after extracting: 78.8 MB.** A procedure specifically used (artificially increasing file size) by criminals to make malware analysis more difficult:

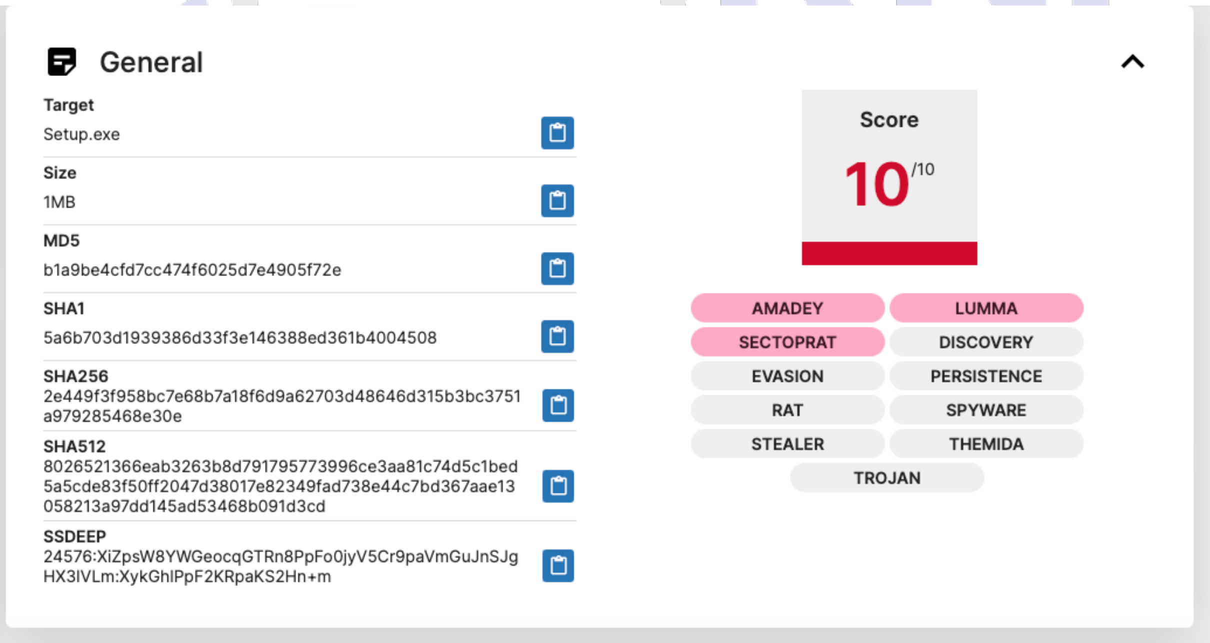


fonts
Images
lang
PIDGENX.DLL
Setup.exe
updates
VCCORLIB140.DLL
Views



Password_1234_Setup 78,8 MB
Zmodyfikowano: Dzisiaj, 12:35

7) **Uploading the .rar file for analysis at Tria.ge**
(full report: https://tria.ge/230726-l1lxjsag48/behavioral2):



General

Target
Setup.exe

Size
1MB

MD5
b1a9be4cfd7cc474f6025d7e4905f72e

SHA1
5a6b703d1939386d33f3e146388ed361b4004508

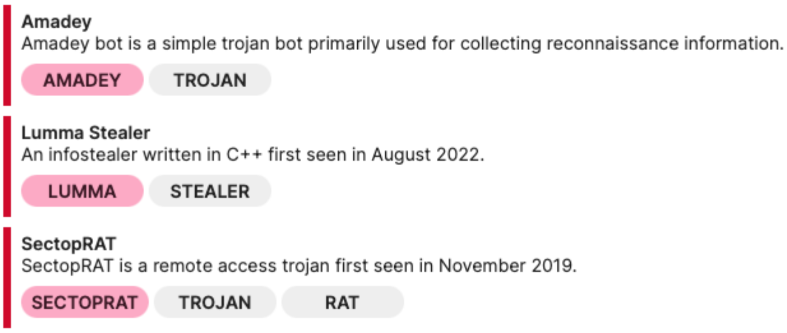
SHA256
2e449f3f958bc7e68b7a18f6d9a62703d48646d315b3bc3751a979285468e30e

SHA512
8026521366eab3263b8d791795773996ce3aa81c74d5c1bed5a5cde83f50ff2047d38017e82349fad738e44c7bd367aae13058213a97dd145ad53468b091d3cd

SSDEEP
24576:XiZpsW8YWGeocqGTRn8PpFo0jyV5Cr9paVmGuJnSJgHX3IVLm:XykGhlPpF2KRpaKS2Hn+m

Score
10/10

8) **The analysis showed that the .exe file contained malware, toiling to steal information from the victim's device, such as:**
- AMADEY
- Stealer LUMMA
- SECTOPRAT

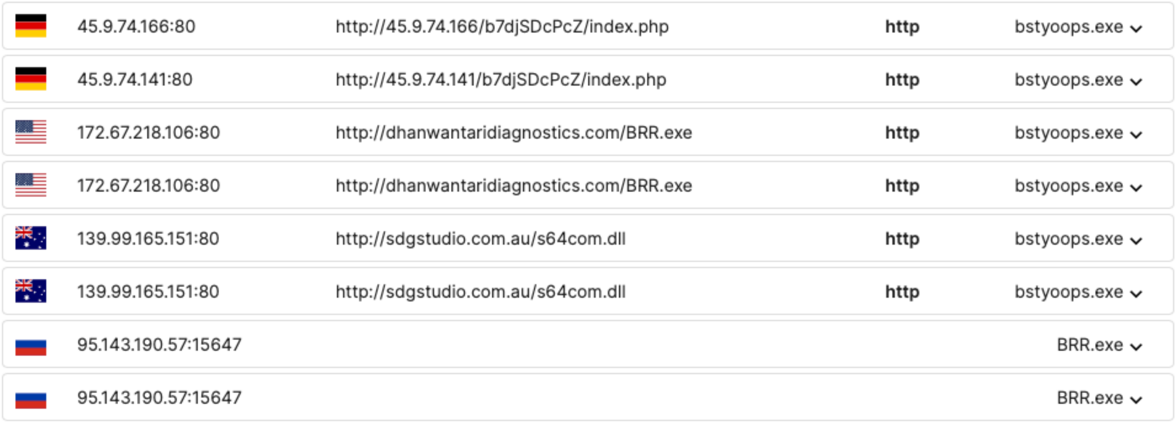


Amadey
Amadey bot is a simple trojan bot primarily used for collecting reconnaissance information.
AMADEY TROJAN

Lumma Stealer
An infostealer written in C++ first seen in August 2022.
LUMMA STEALER

SectopRAT
SectopRAT is a remote access trojan first seen in November 2019.
SECTOPRAT TROJAN RAT

9) **In the next step of the analysis, we checked which addresses the malware connects to when it tries to run:**



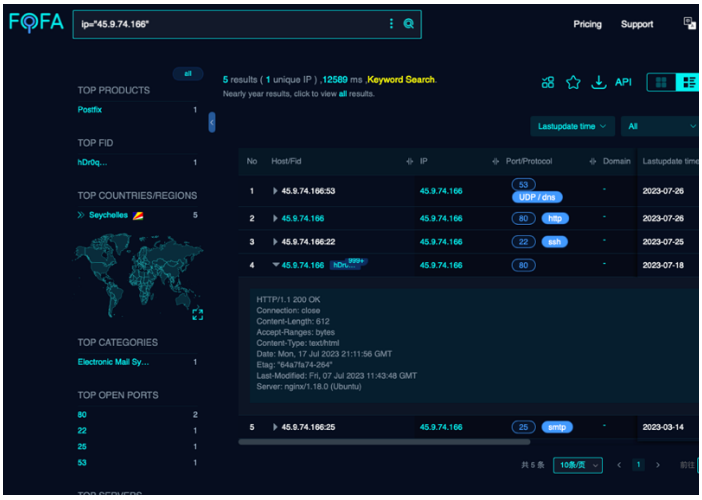
🇩🇪	45.9.74.166:80	http://45.9.74.166/b7djSDcPcZ/index.php	http	bstyoops.exe ⌄
🇩🇪	45.9.74.141:80	http://45.9.74.141/b7djSDcPcZ/index.php	http	bstyoops.exe ⌄
🇺🇸	172.67.218.106:80	http://dhanwantaridiagnostics.com/BRR.exe	http	bstyoops.exe ⌄
🇺🇸	172.67.218.106:80	http://dhanwantaridiagnostics.com/BRR.exe	http	bstyoops.exe ⌄
🇦🇺	139.99.165.151:80	http://sdgstudio.com.au/s64com.dll	http	bstyoops.exe ⌄
🇦🇺	139.99.165.151:80	http://sdgstudio.com.au/s64com.dll	http	bstyoops.exe ⌄
🇷🇺	95.143.190.57:15647			BRR.exe ⌄
🇷🇺	95.143.190.57:15647			BRR.exe ⌄

C2:

45.9.74.166:80
45.9.74.141:80
172.67.218.106:80
139.99.165.151:80
95.143.190.57:15647

a) 45.9.74[.]166

Fofa.info:



5 results (1 unique IP) ,12589 ms ,Keyword Search.
Nearly year results, click to view all results.

TOP PRODUCTS
Postfix 1

TOP FID
hDr0q... 1

TOP COUNTRIES/REGIONS
Seychelles 5

TOP CATEGORIES
Electronic Mail Sy... 1

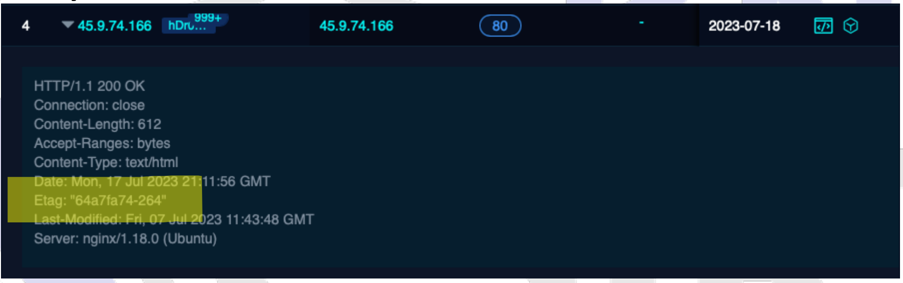
TOP OPEN PORTS
80 2
22 1
25 1
53 1

No	Host/Fid	IP	Port/Protocol	Domain	Lastupdate time
1	45.9.74.166:53	45.9.74.166	53 UDP / dns	-	2023-07-26
2	45.9.74.166	45.9.74.166	80 http	-	2023-07-26
3	45.9.74.166:22	45.9.74.166	22 ssh	-	2023-07-25
4	45.9.74.166 hDr... 999+	45.9.74.166	80	-	2023-07-18
5	45.9.74.166:25	45.9.74.166	25 smtp	-	2023-03-14

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 612
Accept-Ranges: bytes
Content-Type: text/html
Date: Mon, 17 Jul 2023 21:11:56 GMT
Etag: "64a7fa74-264"
Last-Modified: Fri, 07 Jul 2023 11:43:48 GMT
Server: nginx/1.18.0 (Ubuntu)
```

Details of the server's IP address, from which we can find out the value of Etag: **"64a7fa74-264"**

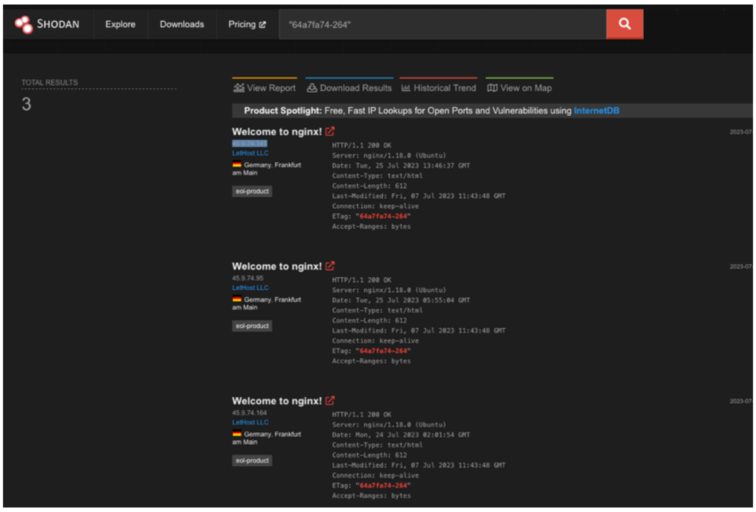
ETag analysis:



4	45.9.74.166 hDr... 999+	45.9.74.166	80	-	2023-07-18

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 612
Accept-Ranges: bytes
Content-Type: text/html
Date: Mon, 17 Jul 2023 21:11:56 GMT
Etag: "64a7fa74-264"
Last-Modified: Fri, 07 Jul 2023 11:43:48 GMT
Server: nginx/1.18.0 (Ubuntu)
```

Checking the Etag value in the Shodan.io tool, from where we can learn about two more IP addresses (the .141 address was already known during the tria.ge malware analysis):
- 45.9.74.141 (https://www.virustotal.com/gui/ip-address/45.9.74.141);
- 45.9.74.95 (https://www.virustotal.com/gui/ip-address/45.9.74.95);
- 45.9.74.164 (https://www.virustotal.com/gui/ip-address/45.9.74.164);



TOTAL RESULTS
3

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

Welcome to nginx!
45.9.74.141
LetHost LLC
Germany, Frankfurt am Main
eol-product

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 25 Jul 2023 13:46:37 GMT
Content-Type: text/html
Content-Length: 612
Last-Modified: Fri, 07 Jul 2023 11:43:48 GMT
Connection: keep-alive
ETag: "64a7fa74-264"
Accept-Ranges: bytes
```

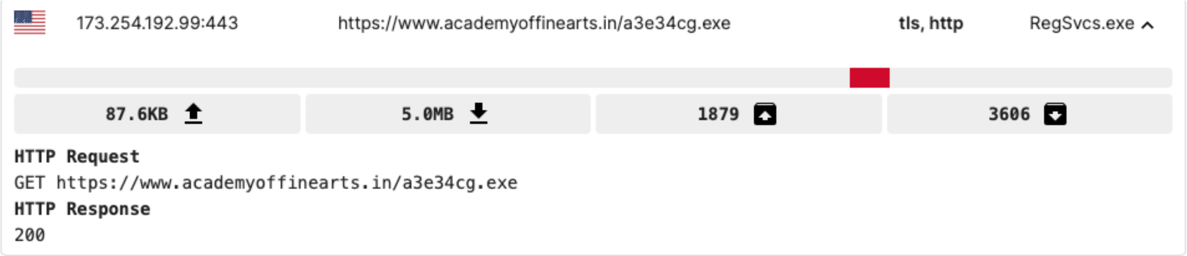
Welcome to nginx!
45.9.74.95
LetHost LLC
Germany, Frankfurt am Main
eol-product

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 25 Jul 2023 05:55:04 GMT
Content-Type: text/html
Content-Length: 612
Last-Modified: Fri, 07 Jul 2023 11:43:48 GMT
Connection: keep-alive
ETag: "64a7fa74-264"
Accept-Ranges: bytes
```

Welcome to nginx!
45.9.74.164
LetHost LLC
Germany, Frankfurt am Main
eol-product

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 24 Jul 2023 02:01:54 GMT
Content-Type: text/html
Content-Length: 612
Last-Modified: Fri, 07 Jul 2023 11:43:48 GMT
Connection: keep-alive
ETag: "64a7fa74-264"
Accept-Ranges: bytes
```

10) Downloading another .exe file from the address with which, the malware contacted:

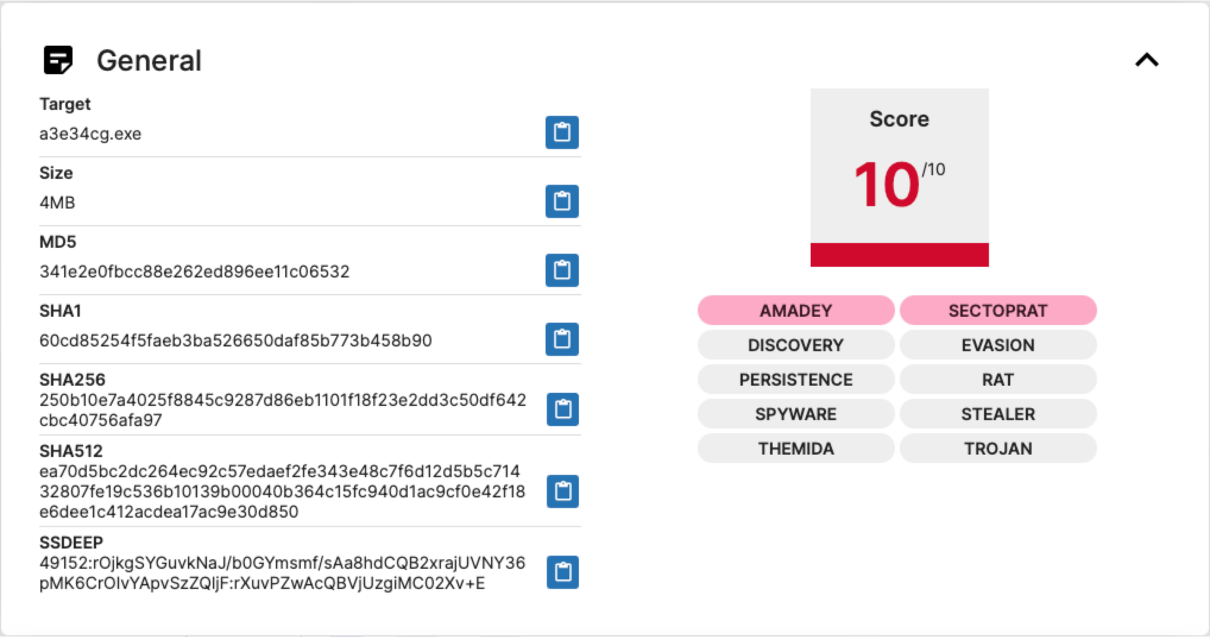


173.254.192.99:443 https://www.academyoffinearts.in/a3e34cg.exe **tls, http** RegSvcs.exe

87.6KB 5.0MB 1879 3606

```
HTTP Request
GET https://www.academyoffinearts.in/a3e34cg.exe
HTTP Response
200
```

11) Analysis of file: a3e34cg.exe in Tria.ge
(full report: https://tria.ge/230726-m6pfasba29/behavioral1):



General

Target
a3e34cg.exe

Size
4MB

MD5
341e2e0fbcc88e262ed896ee11c06532

SHA1
60cd85254f5faeb3ba526650daf85b773b458b90

SHA256
250b10e7a4025f8845c9287d86eb1101f18f23e2dd3c50df642cbc40756afa97

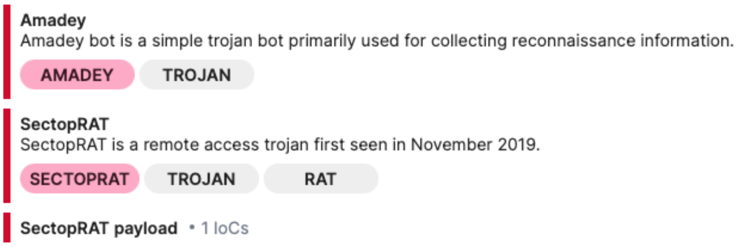
SHA512
ea70d5bc2dc264ec92c57edaef2fe343e48c7f6d12d5b5c71432807fe19c536b10139b00040b364c15fc940d1ac9cf0e42f18e6dee1c412acdea17ac9e30d850

SSDEEP
49152:rOjkgSYGuvkNaJ/b0GYmsmf/sAa8hdCQB2xrajUVNY36pMK6CrOlvYApvSzZQljF:rXuvPZwAcQBVjUzgiMC02Xv+E

Score
10/10

AMADEY SECTOPRAT DISCOVERY EVASION PERSISTENCE RAT SPYWARE STEALER THEMIDA TROJAN

12) **Analysis showed that the a3e34cg.exe file contained malware similar to the previous sample**.
This time there is no - Lumma Stealer:
- AMADEY
- SECTOPRAT

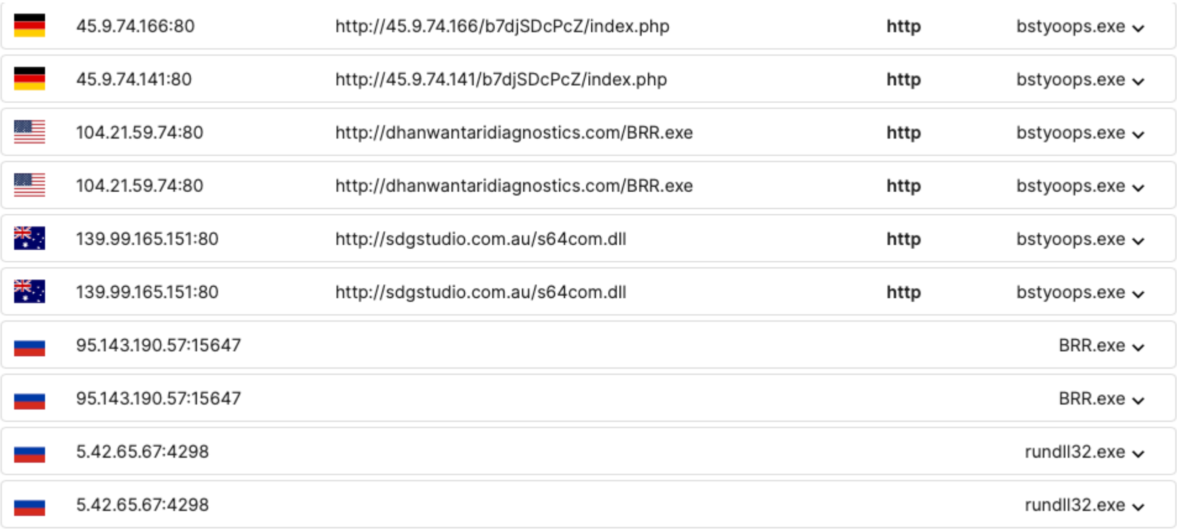


Amadey
Amadey bot is a simple trojan bot primarily used for collecting reconnaissance information.
AMADEY TROJAN

SectopRAT
SectopRAT is a remote access trojan first seen in November 2019.
SECTOPRAT TROJAN RAT

SectopRAT payload • 1 IoCs

13) **Just like when we analyzed the first sample, we will check which IPs the malware is connecting to:**

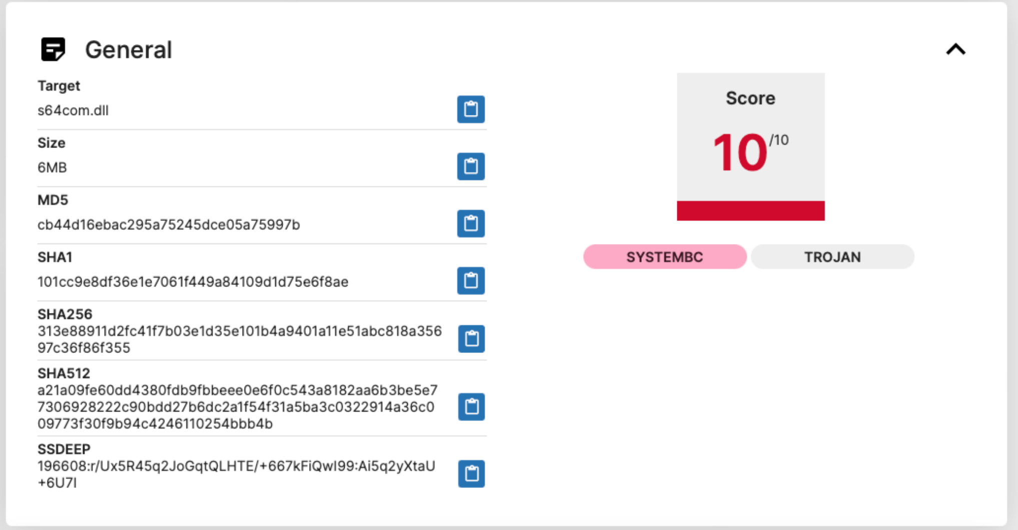


🇩🇪	45.9.74.166:80	http://45.9.74.166/b7djSDcPcZ/index.php	http	bstyoops.exe ⌄
🇩🇪	45.9.74.141:80	http://45.9.74.141/b7djSDcPcZ/index.php	http	bstyoops.exe ⌄
🇺🇸	104.21.59.74:80	http://dhanwantaridiagnostics.com/BRR.exe	http	bstyoops.exe ⌄
🇺🇸	104.21.59.74:80	http://dhanwantaridiagnostics.com/BRR.exe	http	bstyoops.exe ⌄
🇦🇺	139.99.165.151:80	http://sdgstudio.com.au/s64com.dll	http	bstyoops.exe ⌄
🇦🇺	139.99.165.151:80	http://sdgstudio.com.au/s64com.dll	http	bstyoops.exe ⌄
🇷🇺	95.143.190.57:15647			BRR.exe ⌄
🇷🇺	95.143.190.57:15647			BRR.exe ⌄
🇷🇺	5.42.65.67:4298			rundll32.exe ⌄
🇷🇺	5.42.65.67:4298			rundll32.exe ⌄

C2:

45.9.74.166:80
45.9.74.141:80
104.21.59.74:80
139.99.165.151:80
95.143.190.57:15647
5.42.65.67:4298 - **NEW ADDRESS**

14) **In the next step, we took another sample from:** *hxxp://sdgstudio.com[.]au/s64com.dll* and we submitted it for analysis at Tria.ge (full report: https://tria.ge/230726-nhbd7sba78/behavioral1)



General

Target
s64com.dll

Size
6MB

MD5
cb44d16ebac295a75245dce05a75997b

SHA1
101cc9e8df36e1e7061f449a84109d1d75e6f8ae

SHA256
313e88911d2fc41f7b03e1d35e101b4a9401a11e51abc818a356 97c36f86f355

SHA512
a21a09fe60dd4380fdb9fbbeee0e6f0c543a8182aa6b3be5e7 7306928222c90bdd27b6dc2a1f54f31a5ba3c0322914a36c0 09773f30f9b94c4246110254bbb4b

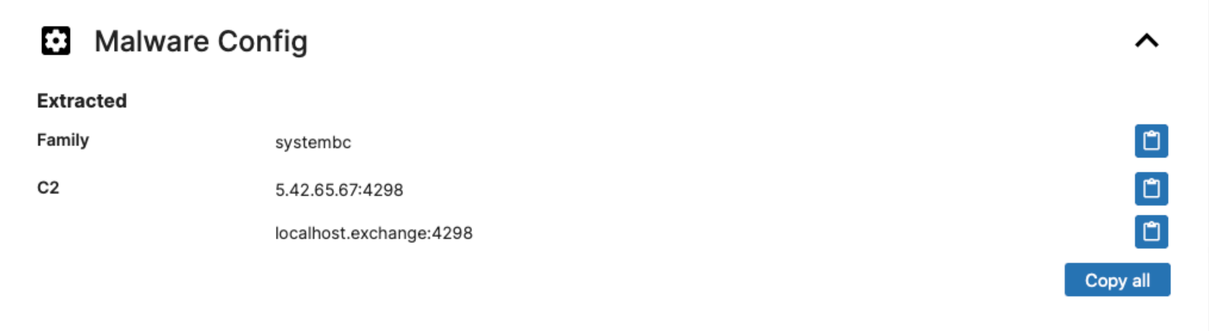
SSDEEP
196608:r/Ux5R45q2JoGqtQLHTE/+667kFiQwI99:Ai5q2yXtaU +6U7I

Score
10/10

SYSTEMBC TROJAN

15) Analysis showed that the s64com.dll file had malware - SystemBC - sewn into it.

IP address: 5.42.65[.]67:4298 was already learned by us during the analysis of the previous sample: a3e34cg.exe (https://www.virustotal.com/gui/ip-address/5.42.65.67/relations).

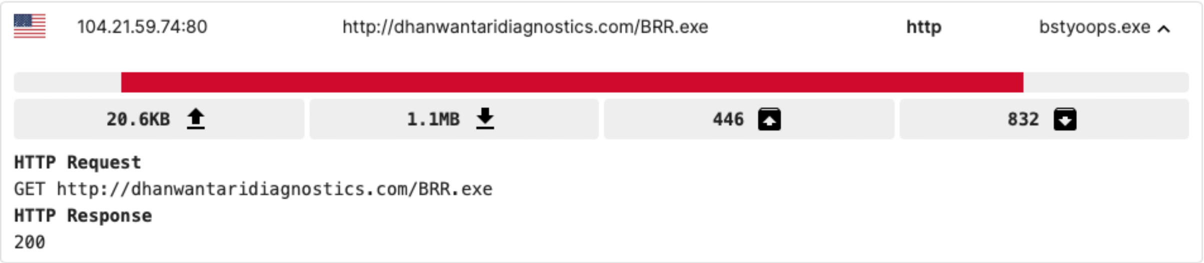


Malware Config

Extracted

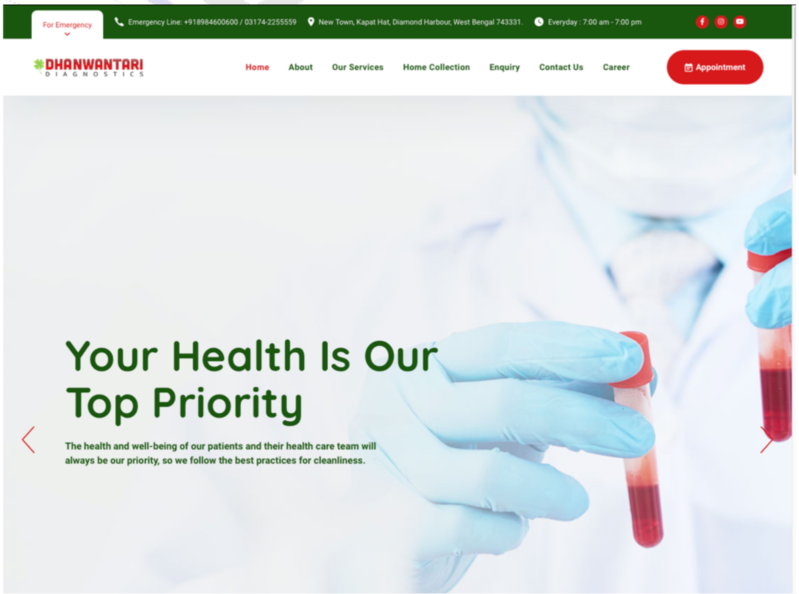
Family	systembc
C2	5.42.65.67:4298
	localhost.exchange:4298

16) Another sample that was analyzed and comes from the same campaign is the file: BRR.exe, hosted at: hxxp://dhanwantaridiagnostics[.]com/BRR.exe



```
104.21.59.74:80    http://dhanwantaridiagnostics.com/BRR.exe    http    bstyoops.exe
20.6KB    1.1MB    446    832
HTTP Request
GET http://dhanwantaridiagnostics.com/BRR.exe
HTTP Response
200
```

The site: hxxp://dhanwantaridiagnostics[.]com was used by criminals as C2 to host malware. The appearance of the listed site:



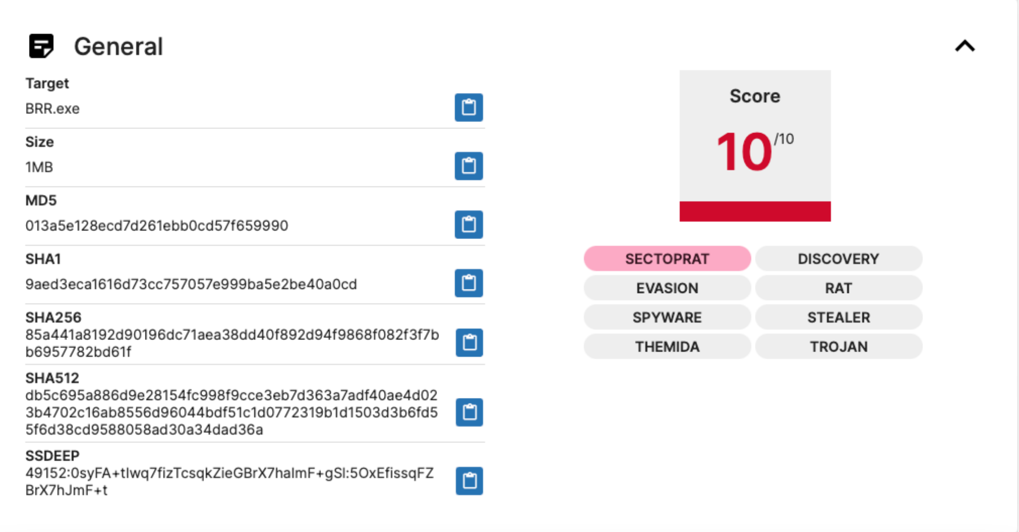
For Emergency
Emergency Line: +918984600600 / 03174-2255559
New Town, Kapat Hat, Diamond Harbour, West Bengal 743331.
Everyday : 7:00 am - 7:00 pm
DHANWANTARI DIAGNOSTICS
Home
About
Our Services
Home Collection
Enquiry
Contact Us
Career
Appointment

Your Health Is Our Top Priority

The health and well-being of our patients and their health care team will always be our priority, so we follow the best practices for cleanliness.

17) Analysis of theBRR.exe file in Tria.ge

(full report: https://tria.ge/230726-nx5xcsbb65/behavioral1):



General

Target
BRR.exe

Size
1MB

MD5
013a5e128ecd7d261ebb0cd57f659990

SHA1
9aed3eca1616d73cc757057e999ba5e2be40a0cd

SHA256
85a441a8192d90196dc71aea38dd40f892d94f9868f082f3f7bb6957782bd61f

SHA512
db5c695a886d9e28154fc998f9cce3eb7d363a7adf40ae4d023b4702c16ab8556d96044bdf51c1d0772319b1d1503d3b6fd55f6d38cd9588058ad30a34dad36a

SSDEEP
49152:0syFA+tlwq7fizTcsqkZieGBrX7halmF+gSl:5OxEfissqFZBrX7hJmF+t

Score
10/10

18) The analysis showed that the BRR.EXE file had malware - SECTOPRAT - sewn into it.

The IP address to which the aforementioned sample connects is 95.143.190.57:15647 was already learned by us during the analysis of the source sample: Setup.exe (https://www.virustotal.com/gui/ip-address/95.143.190.57).

Summary

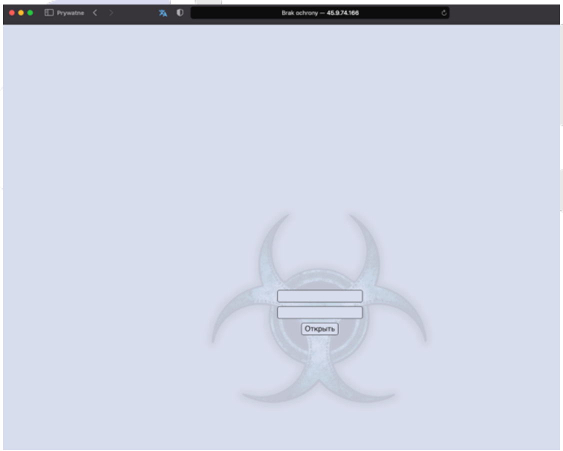
This malware analysis report provides detailed information on cybercriminal activity carried out on the YouTube platform. In particular, it focuses on the malware distribution method of including download links in video descriptions.

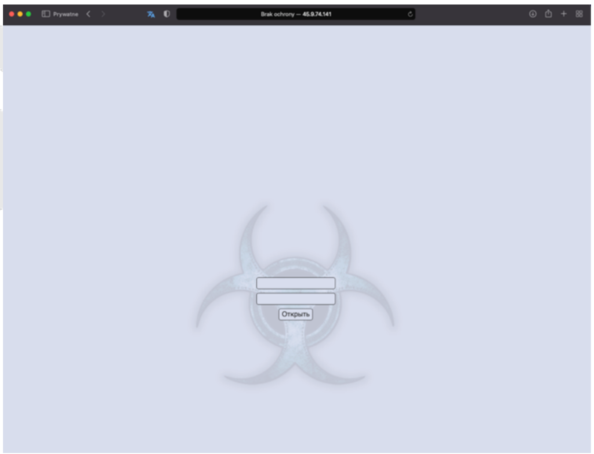
The investigation involved downloading and analyzing files that were found to contain various types of malware, including some that focus on stealing information from the victim's device.

ETag analysis was able to identify more IP addresses that could be used for the same purpose. Each of the malicious files communicated with two common IP addresses.

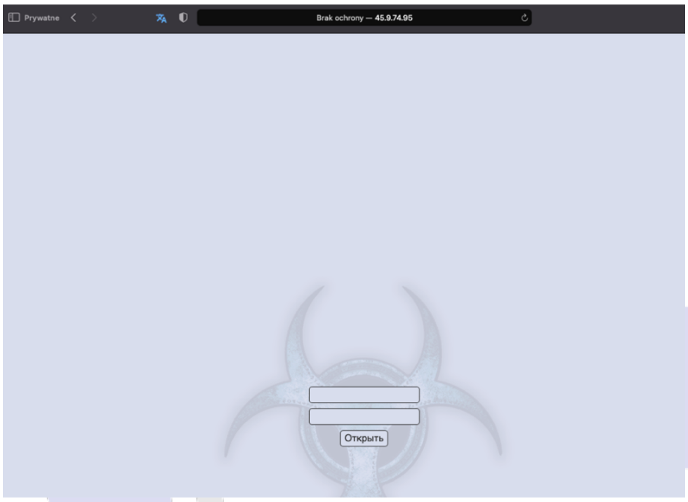
<u>These are the addresses:</u>
hxxp://45.9.74[.]141/b7djSDcPcZ/index.php
hxxp://45.9.74[.]166/b7djSDcPcZ/index.php

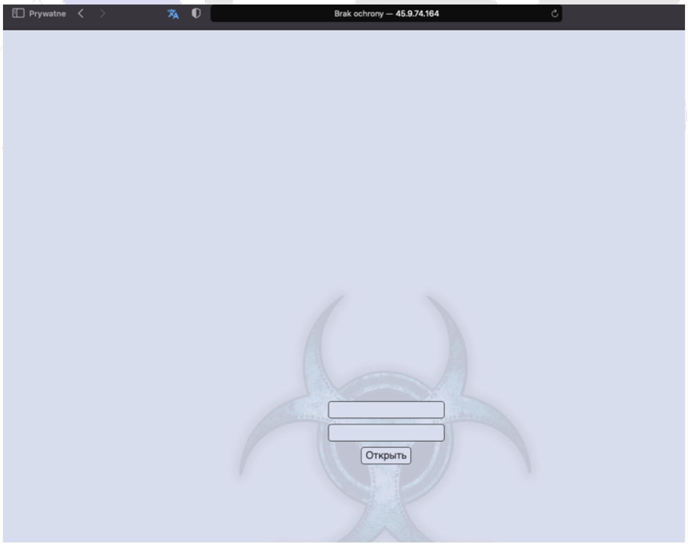
At the above addresses, we can find the AmadeyBot login panel:





Analysis and a search by ETag values found more addresses:
- 45.9.74[.]95/b7djSDcPcZ/Login.php (https://www.virustotal.com/gui/ip-address/45.9.74.95);
- 45.9.74[.]164/ b7djSDcPcZ/Login.php (https://www.virustotal.com/gui/ip-address/45.9.74.164);
- http://45.9.74[.]119/b7djSDcPcZ/Login.php (https://www.virustotal.com/gui/ip-address/45.9.74.119);





Shodan query:
```
"64a7fa74-264"
```

Fuzzing results of the above addresses:
```
hxxp://45.9.74[.]164/files.rar
hxxp://45.9.74[.]141/files.rar
hxxp://45.9.74[.]119/files.rar
```