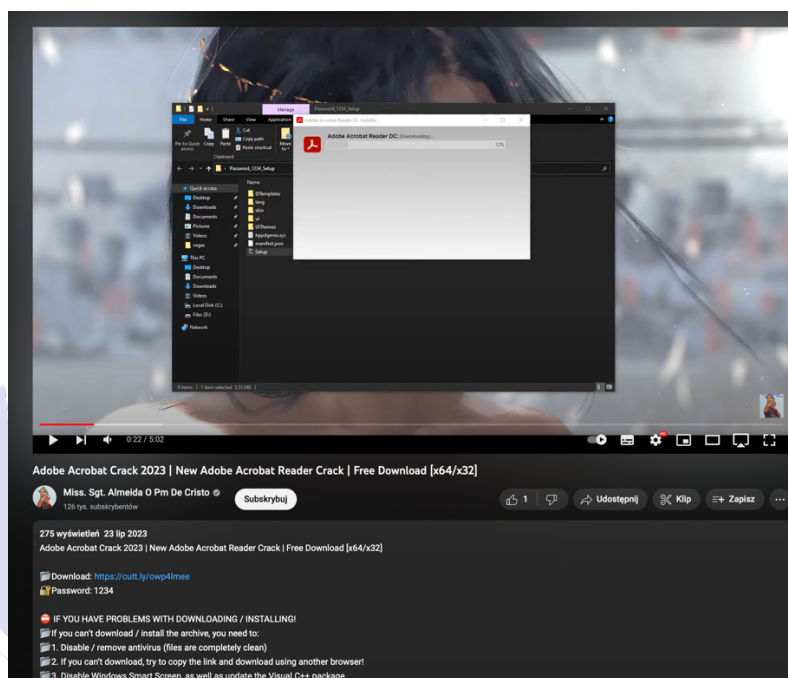


## Analiza złośliwego oprogramowania z serwisu YouTube

### Opis analizy:

Raport ten stanowi analizę złośliwego oprogramowania znalezionej na platformie YouTube. Skupia się na konkretnym przypadku, w którym został użyty link do pobrania z opisu filmu, reklamującego oprogramowanie typu crack do popularnej aplikacji Acrobat Reader. Po pobraniu i analizie zawartości pliku .rar, stwierdzono, że zawiera on złośliwe oprogramowanie skupiające się na kradzieży informacji z urządzenia ofiary.

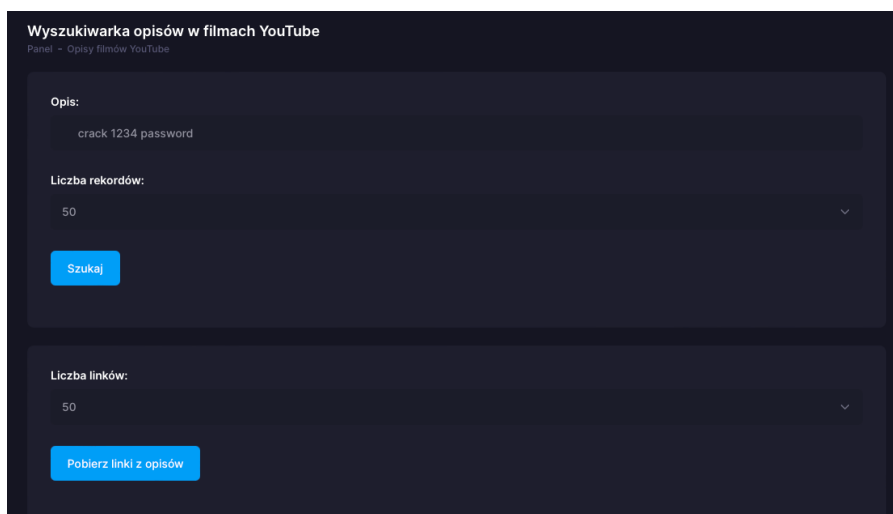


Raport zawiera również informacje o zlokalizowanych adresach IP, do których łączyło się złośliwe oprogramowanie. Analizowane są kolejne pliki .exe, które były pobierane i kontaktowały się z tymi samymi adresami IP. Analizy wykazały obecność tych samych rodzajów złośliwego oprogramowania, z kilkoma dodatkowymi typami odkrytymi w trakcie badania.

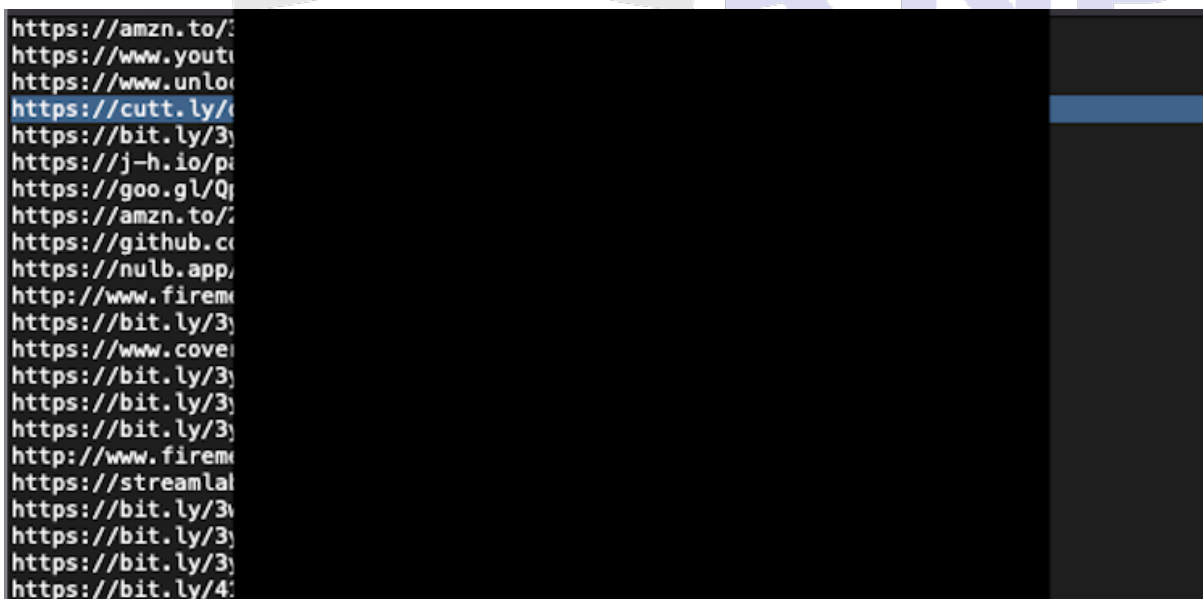
Raport podkreśla, że wszystkie zbadane złośliwe pliki komunikowały się z dwoma wspólnymi adresami IP. Dodatkowo, za pomocą analizy ETag, udało się zlokalizować kolejne adresy IP, które mogą być wykorzystywane do tego samego celu.

Dokument opisuje proces identyfikacji i analizy złośliwego oprogramowania, wykazując kroki, które zostały podjęte w celu zidentyfikowania i zrozumienia działania tego oprogramowania, jak również jego punktów komunikacyjnych w formie adresów IP.

- 1) Szukanie malware na platformie Youtube pod frazę kluczową: „password 1234 crack”:

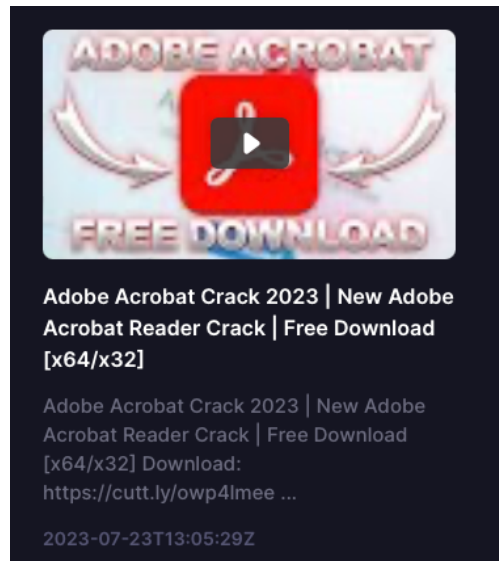


- 2) Pobranie linków z opisów oraz wybranie jednego w celu analizy:

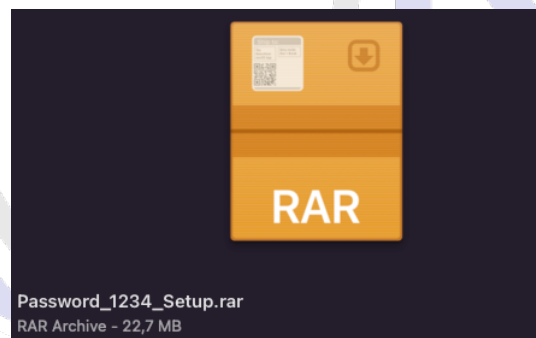


[TLP:CLEAR]

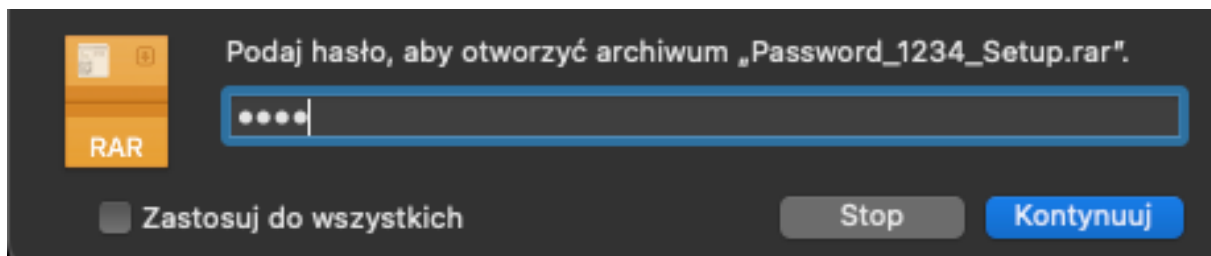
- 3) **Link do pobrania oprogramowania typu crack do popularnej aplikacji: Acrobat Reader** (film na Youtube opublikowany 23.07.2023 roku):



- 4) **Pobranie pliku o rozszerzeniu .rar z linku z opisu filmu:**

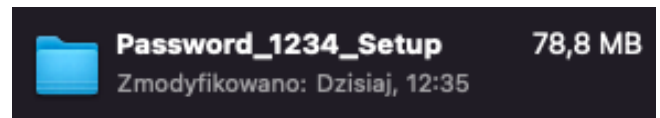
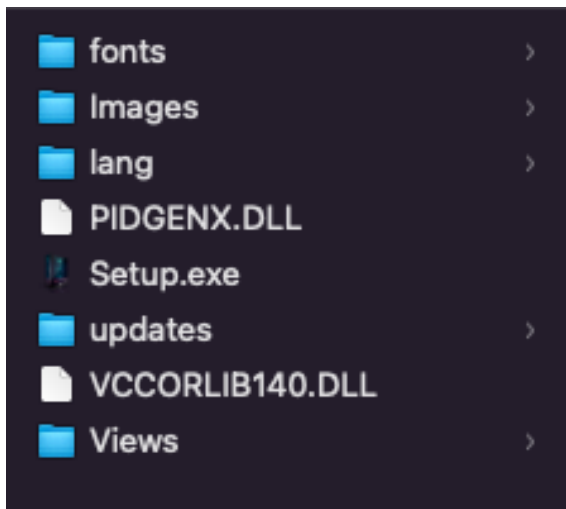


- 5) **Wpisanie hasła z opisu filmu do archiwum oraz rozpakowanie zawartości:**

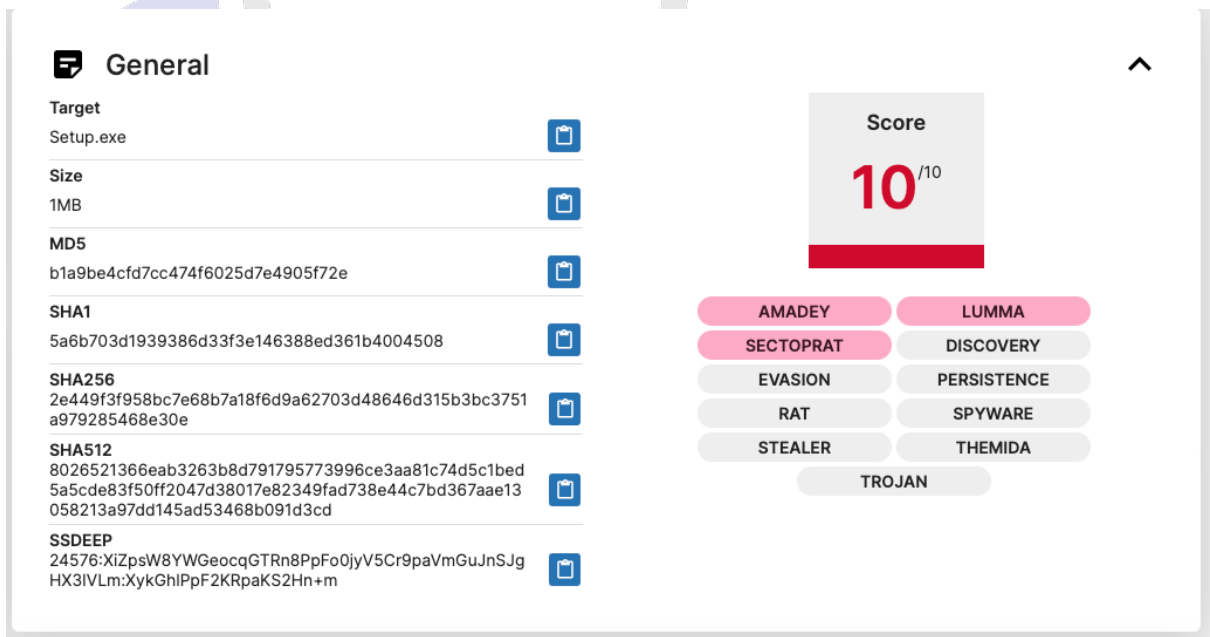


[TLP:CLEAR]

- 6) **Zawartość archiwum .rar. Rozmiar po wypakowaniu: 78.8 MB.** Zabieg specjalnie wykorzystywany (sztuczne powiększanie rozmiaru plików) przez przestępców w celu utrudnienia analizy złośliwego oprogramowania:



- 7) **Przesłanie pliku .rar do analizy w serwisie Tria.ge**  
(cały raport: <https://tria.ge/230726-l1lxjsag48/behavioral2>):



**General**

Target  
Setup.exe

Size  
1MB

MD5  
b1a9be4cfd7cc474f6025d7e4905f72e

SHA1  
5a6b703d1939386d33f3e146388ed361b4004508

SHA256  
2e449f3f958bc7e68b7a18f6d9a62703d48646d315b3bc3751a979285468e30e

SHA512  
8026521366eab3263b8d791795773996ce3aa81c74d5c1bed5a5cde83f50ff2047d38017e82349fad738e44c7bd367aae13058213a97dd145ad53468b091d3cd

SSDEEP  
24576:XiZpsW8YWGeocqGTRn8PpFo0jyV5Cr9paVmGuJnSjgHX3iVLm:XykGhIPpF2KRpaKS2Hn+m

**Score**  
**10**<sup>/10</sup>

AMADEY LUMMA  
SECTOPRAT DISCOVERY  
EVASION PERSISTENCE  
RAT SPYWARE  
STEALER THEMIDA  
TROJAN

**8) Analiza wykazała, że w pliku .exe znajdują się złośliwe oprogramowania, trudniące się m.in. w kradzieży informacji z urządzenia ofiary, takie jak:**

- 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

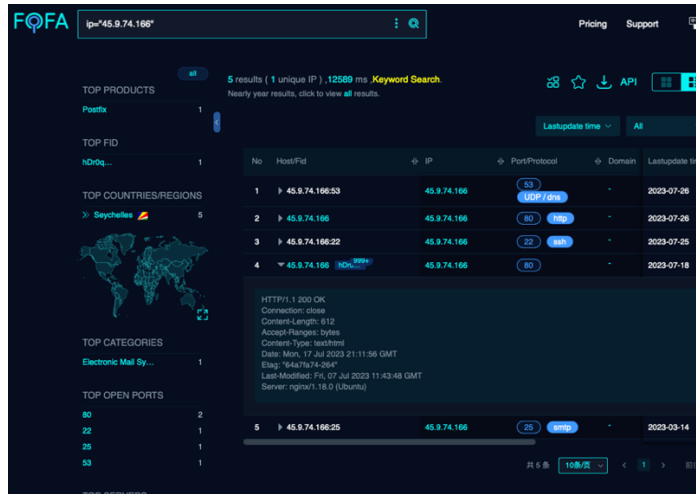
**9) W kolejnym kroku analizy sprawdziliśmy, do jakich adresów łączy się złośliwe oprogramowanie podczas próby uruchomienia:**

	45.9.74.166:80	http://45.9.74.166/b7djSDcPcZ/index.php	http	bstyoops.exe v
	45.9.74.141:80	http://45.9.74.141/b7djSDcPcZ/index.php	http	bstyoops.exe v
	172.67.218.106:80	http://dhanwantaridiagnostics.com/BRR.exe	http	bstyoops.exe v
	172.67.218.106:80	http://dhanwantaridiagnostics.com/BRR.exe	http	bstyoops.exe v
	139.99.165.151:80	http://sdgstudio.com.au/s64com.dll	http	bstyoops.exe v
	139.99.165.151:80	http://sdgstudio.com.au/s64com.dll	http	bstyoops.exe v
	95.143.190.57:15647			BRR.exe v
	95.143.190.57:15647			BRR.exe v

**C2:**

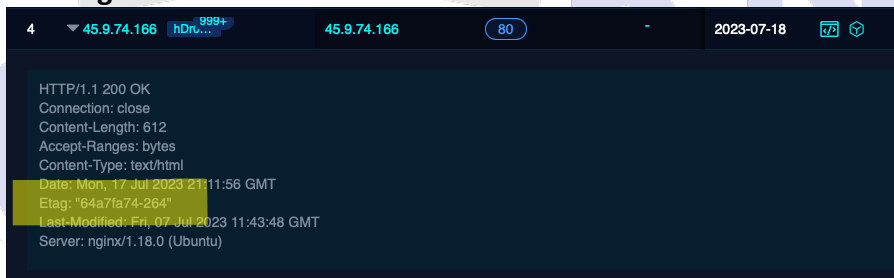
45.9.74.166:80
45.9.74.141:80
172.67.218.106:80
139.99.165.151:80
95.143.190.57:15647

a) 45.9.74[.]166  
Fofa.info:



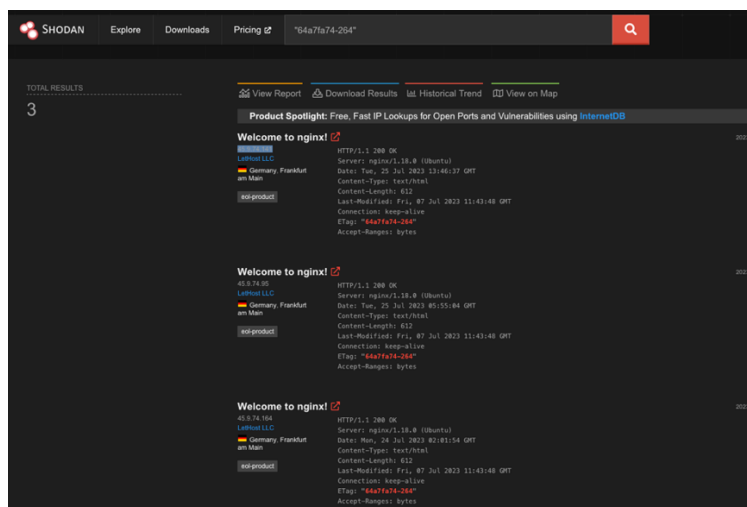
Szczegóły adresu IP serwera, z których możemy się dowiedzieć o wartości Etag: "64a7fa74-264"

Analiza ETag:

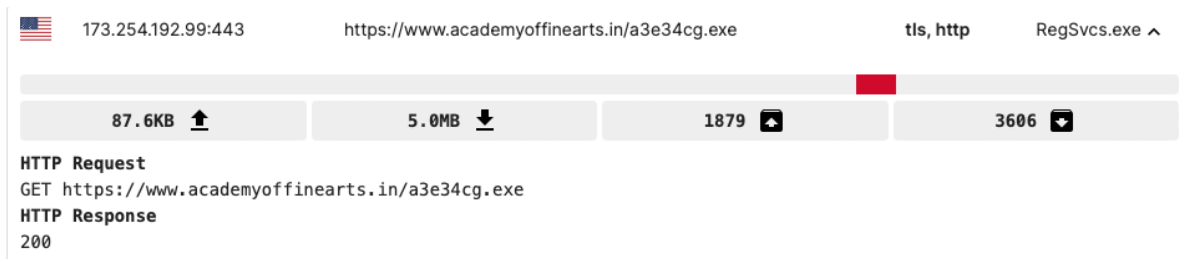


Sprawdzenie wartości Etag w narzędziu Shodan.io, skąd możemy się dowiedzieć o kolejnych dwóch adresach IP (adres .141 był już znany podczas analizy malware w tria.ge):

- 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>);



## 10) Pobranie kolejnego pliku .exe z adresu z którym, kontaktował się malware:



173.254.192.99:443    https://www.academyoffinearts.in/a3e34cg.exe    tls, http    RegSvc.exe ^

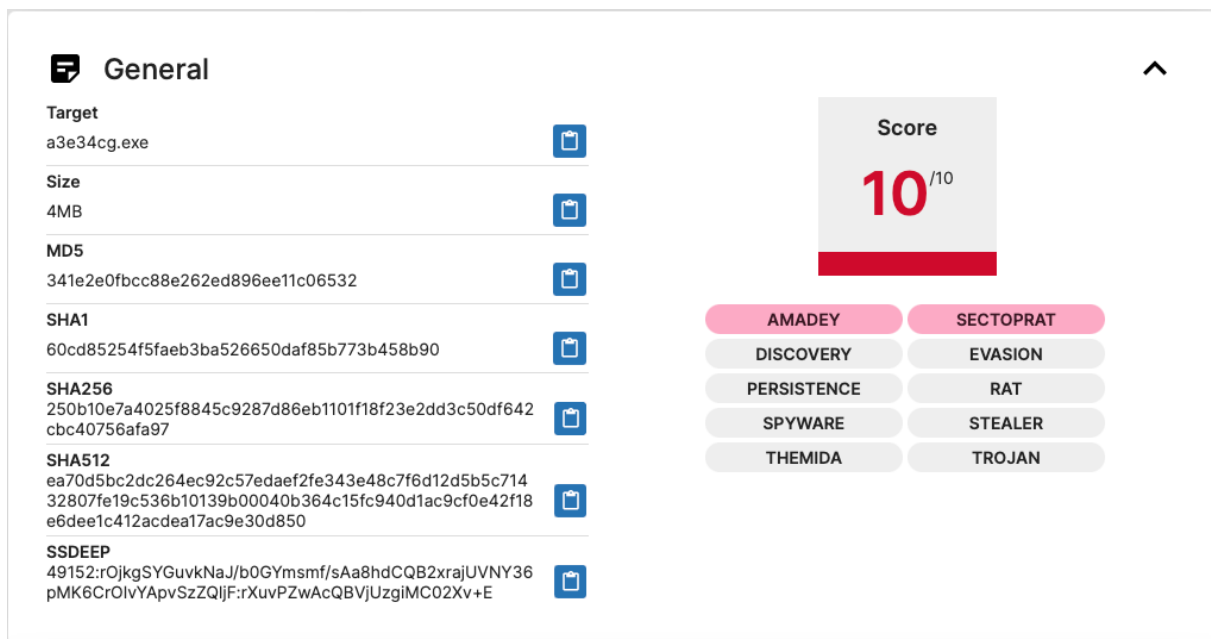
87.6KB ↑    5.0MB ↓    1879 📄    3606 📄

**HTTP Request**  
GET https://www.academyoffinearts.in/a3e34cg.exe

**HTTP Response**  
200

## 11) Analiza pliku: a3e34cg.exe w Tria.ge

(cały raport: <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<sup>10</sup>

**AMADEY**    **SECTOPRAT**

DISCOVERY    EVASION

PERSISTENCE    RAT

SPYWARE    STEALER

THEMIDA    TROJAN

## 12) Analiza wykazała, że w pliku a3e34cg.exe znajdują się złośliwe oprogramowania, podobne jak w poprzedniej próbce.

Tym razem brak – Lumma Stealer’a:

- 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) Tak samo jak podczas analizy pierwszej próbki, sprawdzimy z jakimi IP łączy się złośliwe oprogramowanie:

	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 – <b>NOWY ADRES</b>

14) W kolejnym kroku pobraliśmy kolejną próbkę z:

*hxxp://sdgstudio.com[.]au/s64com.dll* oraz przesłaliśmy ją do analizy w Tria.ge (cały raport: <https://tria.ge/230726-nhbd7sba78/behavioral1>)

**General**

Target  
s64com.dll

Size  
6MB

MD5  
cb44d16ebac295a75245dce05a75997b

SHA1  
101cc9e8df36e1e7061f449a84109d1d75e6f8ae

SHA256  
313e88911d2fc41f7b03e1d35e101b4a9401a11e51abc818a35697c36f86f355

SHA512  
a21a09fe60dd4380fdb9fbbeee0e6f0c543a8182aa6b3be5e77306928222c90bdd27b6dc2a1f54f31a5ba3c0322914a36c009773f30f9b94c4246110254bbb4b

SSDEEP  
196608:r/Ux5R45q2JoGqtQLHTE/+667kFiQwI99:AI5q2yXtaU+6U7I

Score

**10** /10

SYSTEMBC TROJAN






**15) Analiza wykazała, że w pliku s64com.dll zaszyte jest złośliwe oprogramowanie – SystemBC.**

Adres IP: 5.42.65.[.]67:4298 został już przez nas poznany w trakcie analizy poprzedniej próbki: 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	

[Copy all](#)

**16) Kolejną próbką, która została przeanalizowana i pochodzi z tej samej kampanii jest plik: BRR.exe, hostowany na: hxxp://dhanwantaridiagnostics[.]com/BRR.exe**

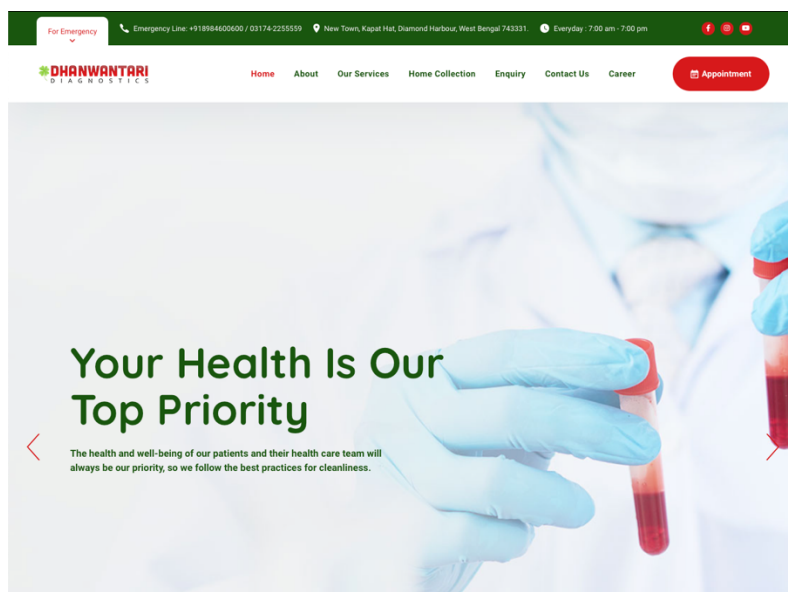
🇺🇸 104.21.59.74:80     
 <http://dhanwantaridiagnostics.com/BRR.exe>     
 http     
 bstyoops.exe ^

---

20.6KB 
1.1MB 
446 
832 

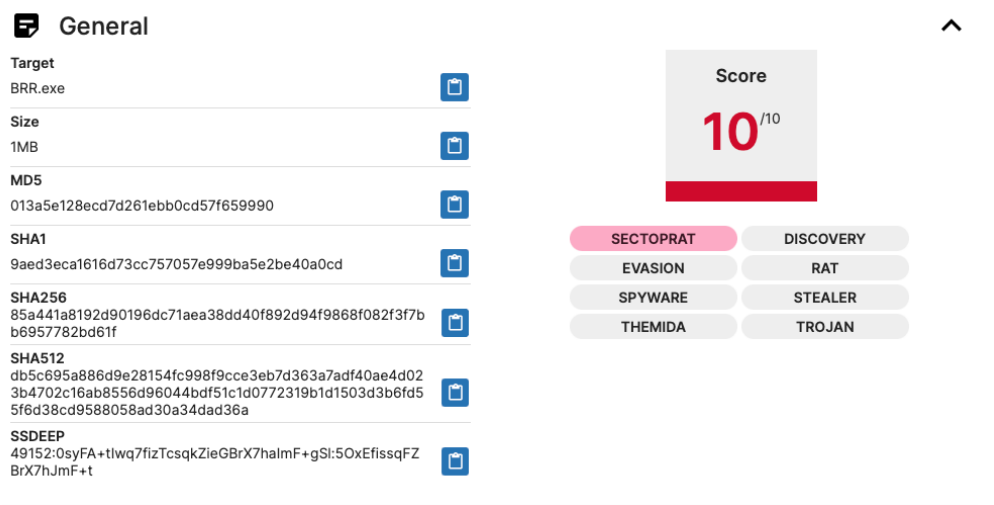
**HTTP Request**  
 GET http://dhanwantaridiagnostics.com/BRR.exe  
**HTTP Response**  
 200

Strona: [hxxp://dhanwantaridiagnostics\[.\]com](http://dhanwantaridiagnostics.com) została wykorzystana przez przestępców jako C2 do hostowania złośliwego oprogramowania. Wygląd wymienionej strony:



### 17) Analiza pliku BRR.exe w Tria.ge

(cały raport: <https://tria.ge/230726-nx5xcsbb65/behavioral1>):



**General**

Target  
BRR.exe

Size  
1MB

MD5  
013a5e128ecd7d261ebb0cd57f659990

SHA1  
9aed3eca1616d73cc757057e999ba5e2be40a0cd

SHA256  
85a441a8192d90196dc71aea38dd40f892d94f9868f082f3f7b  
b6957782bd61f

SHA512  
db5c695a886d9e28154fc998f9cce3eb7d363a7adf40ae4d02  
3b4702c16ab8556d96044bdf51c1d0772319b1d1503d3b6fd5  
5f6d38cd9588058ad30a34dad36a

SSDEEP  
49152:0syFA+tlwq7fizTcsqkZieGbrX7halmF+gSl:5OxEfissqFZ  
BrX7hJmF+t

Score  
**10** /10

SECTOPRAT (highlighted)  
DISCOVERY  
EVASION  
RAT  
SPYWARE  
STEALER  
THEMIDA  
TROJAN

### 18) Analiza wykazała, że w pliku BRR.EXE zaszyte jest złośliwe oprogramowanie – SECTOPRAT.

Adres IP z którym łączy się ww. próbka to 95.143.190.57:15647 został już przez nas poznany w trakcie analizy źródłowej próbki: Setup.exe (<https://www.virustotal.com/gui/ip-address/95.143.190.57>).

## Podsumowanie

Ten raport z analizy złośliwego oprogramowania dostarcza szczegółowe informacje na temat działalności cyberprzestępczej prowadzonej na platformie YouTube. Szczególnie skupia się na metodzie dystrybucji złośliwego oprogramowania, polegającej na umieszczaniu linków do pobrania w opisach filmów.

Badanie obejmowało pobieranie i analizę plików, które okazały się zawierać różne rodzaje złośliwego oprogramowania, w tym takie, które skupiają się na kradzieży informacji z urządzenia ofiary.

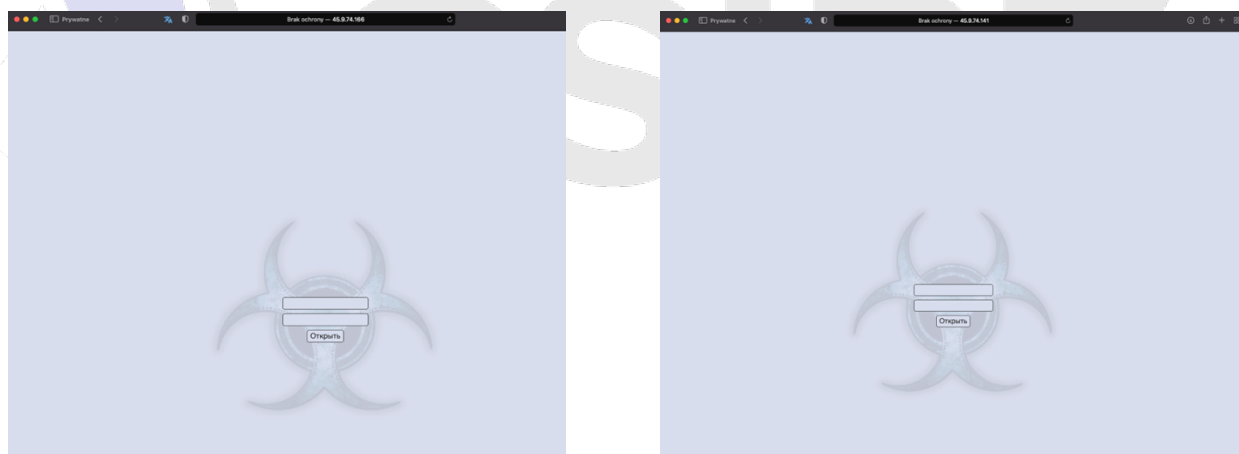
Dzięki analizie ETag udało się zidentyfikować więcej adresów IP, które mogą być wykorzystywane do tego samego celu. Każde ze złośliwych plików komunikowało się z dwoma wspólnymi adresami IP.

Są to adresy:

hxxp://45.9.74[.]141/b7djSDcPcZ/index.php

hxxp://45.9.74[.]166/b7djSDcPcZ/index.php

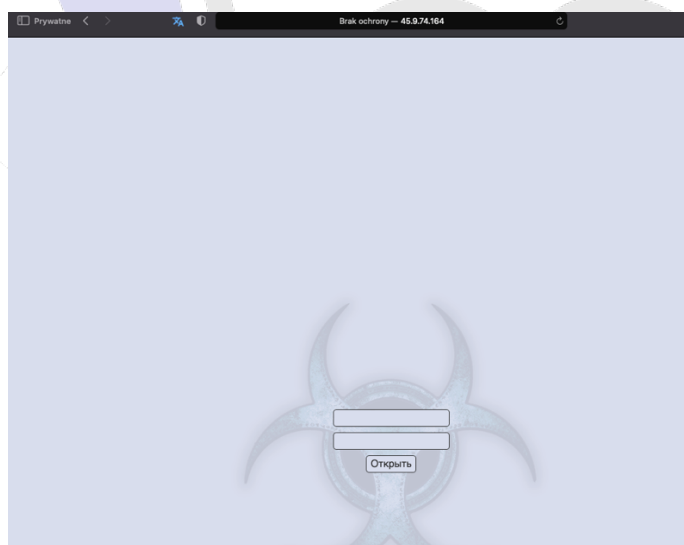
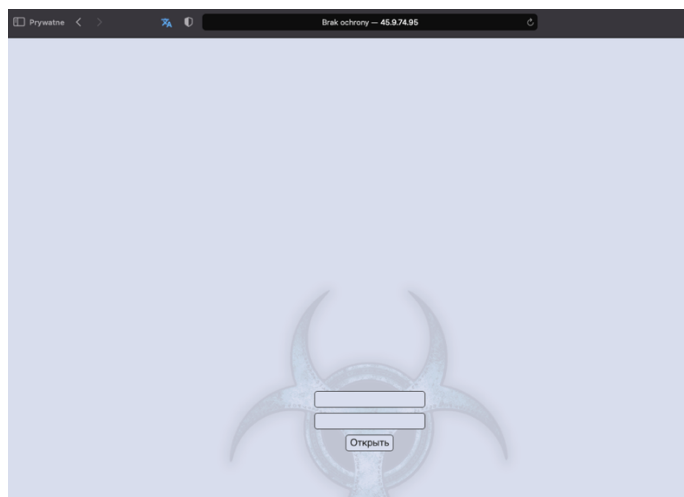
Pod ww. adresami możemy znaleźć panel logowania do AmadeyBot:



[TLP:CLEAR]

**Analiza oraz wyszukiwanie po wartościach ETag pozwoliła znaleźć kolejne adresy:**

- 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"

**Wyniki Fuzzowania powyższych adresów:**

- hxxp://45.9.74[.]164/files.rar
- hxxp://45.9.74[.]141/files.rar
- hxxp://45.9.74[.]119/files.rar