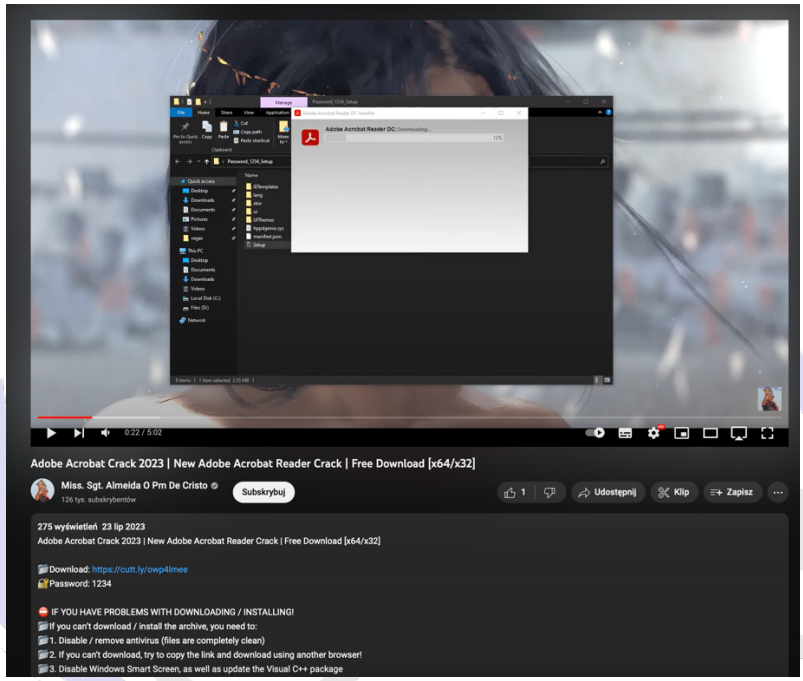
Analiza złośliwego oprogramowania z serwisu YouTube

Opis analizy:

Raport ten stanowi analizę złośliwego oprogramowania znalezionego 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.

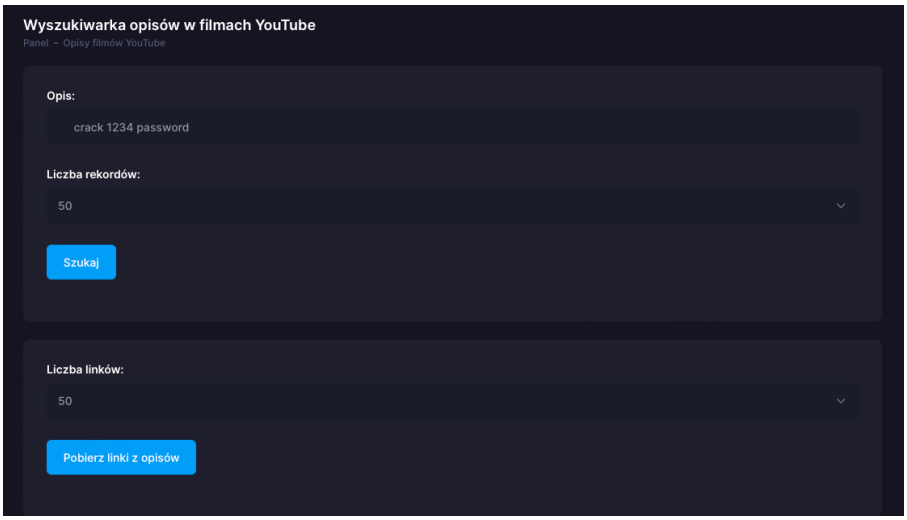


Raport zawiera również informacje o zlokalizowanych adresach IP, do których łączyło się złośliwe oprogramowanie. Analizowane są kolejne pliki .exe, które były pobierane i kontaktowały się z tymi samymi adresami IP. Analizy wykazały obecność tych samych rodzajów złośliwego oprogramowania, z kilkoma dodatkowymi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

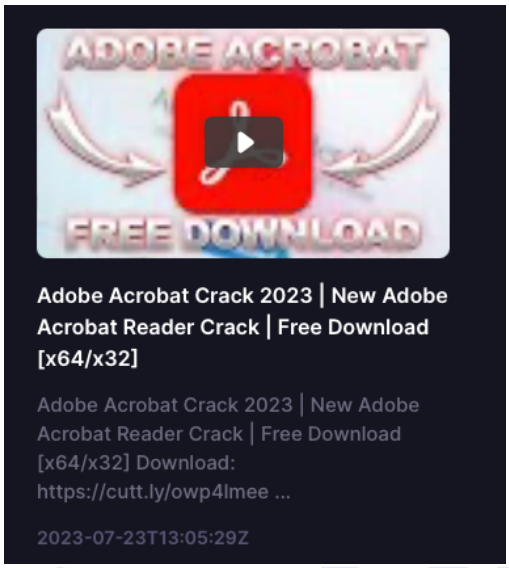
Dokument opisuje proces identyfikacji i analizy złośliwego oprogramowania, wykazując kroki, które zostały podjęte w celu zidentyfikowania i zrozumienia działania tego oprogramowania, jak również jego punktów komunikacyjnych w formie adresów IP.

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

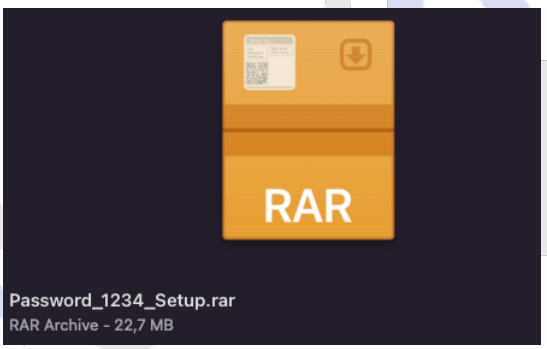


2) **Pobranie linków z opisów oraz wybranie jednego w celu analizy:**

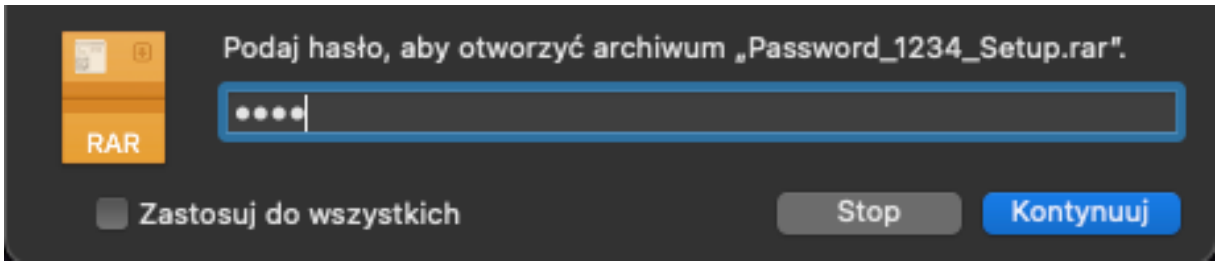
3) **Link do pobrania oprogramowania typu crack do popularnej aplikacji: Acrobat Reader** (film na Youtube opublikowany 23.07.2023 roku):



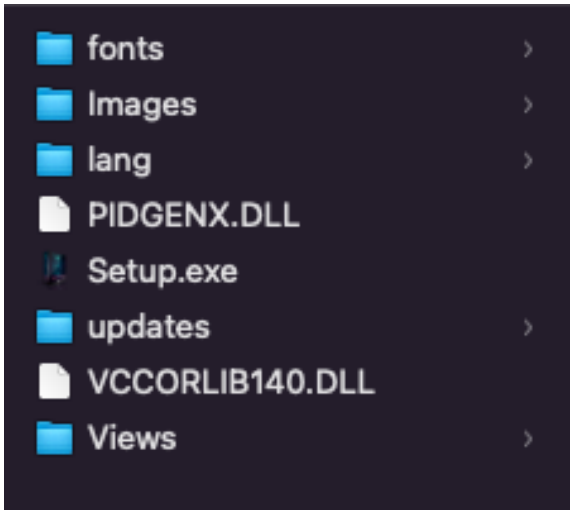
4) **Pobranie pliku o rozszerzeniu .rar z linku z opisu filmu:**

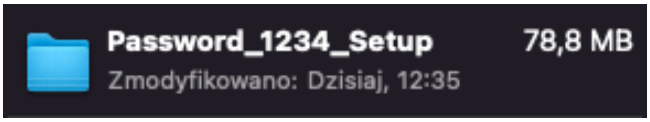


5) **Wpisanie hasła z opisu filmu do archiwum oraz rozpakowanie zawartości:**

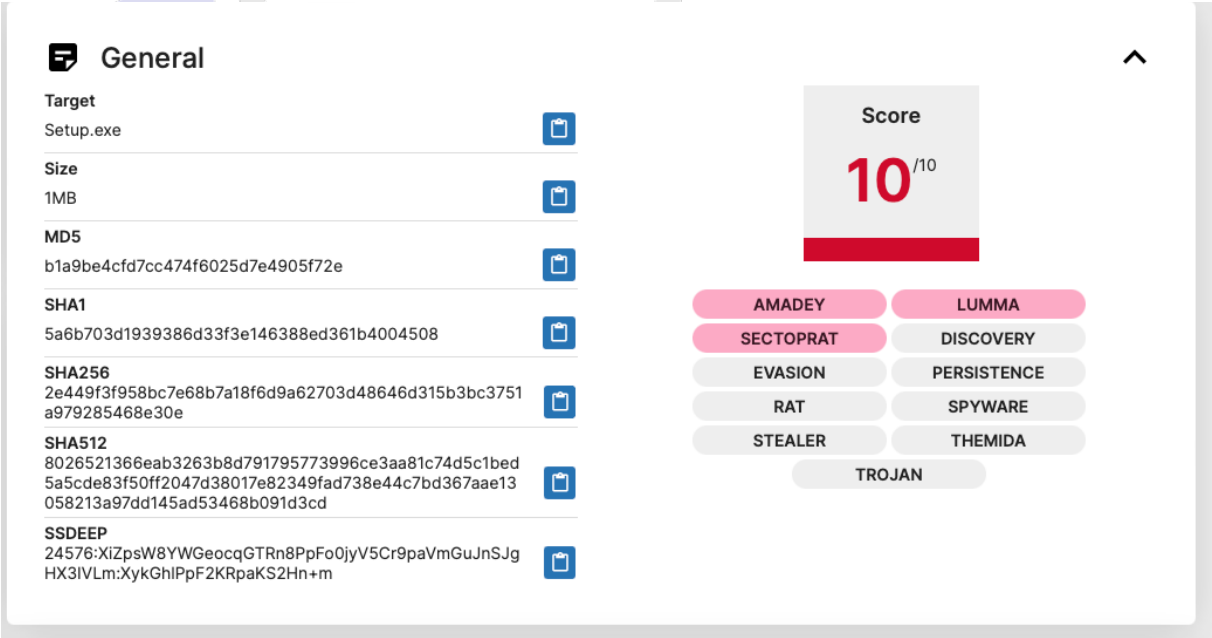


6) **Zawartość archiwum .rar. Rozmiar po wypakowaniu: 78.8 MB.** Zabieg specjalnie wykorzystywany (sztuczne powiększanie rozmiaru plików) przez przestępców w celu utrudnienia analizy złośliwego oprogramowania:

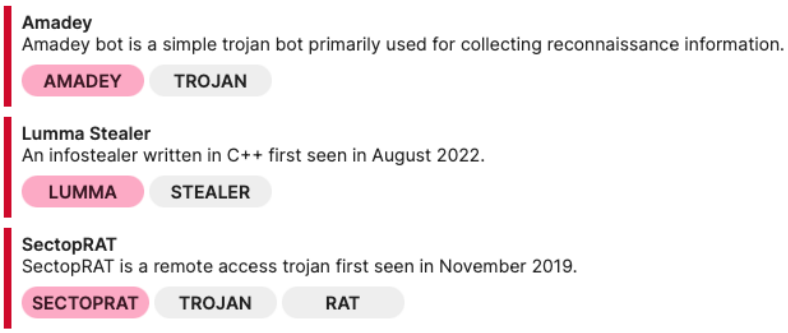




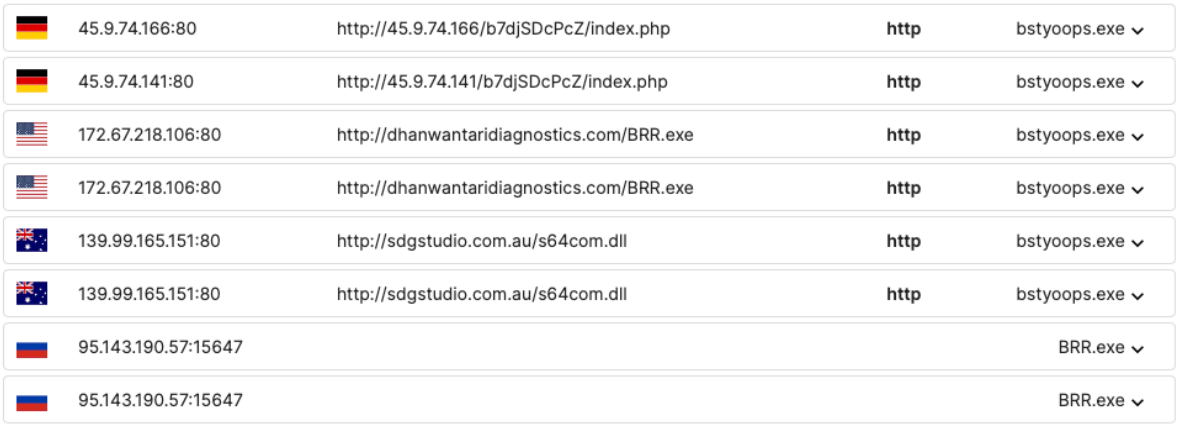
7) **Przesłanie pliku .rar do analizy w serwisie Tria.ge** (cały raport: https://tria.ge/230726-l1lxjsag48/behavioral2):



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



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

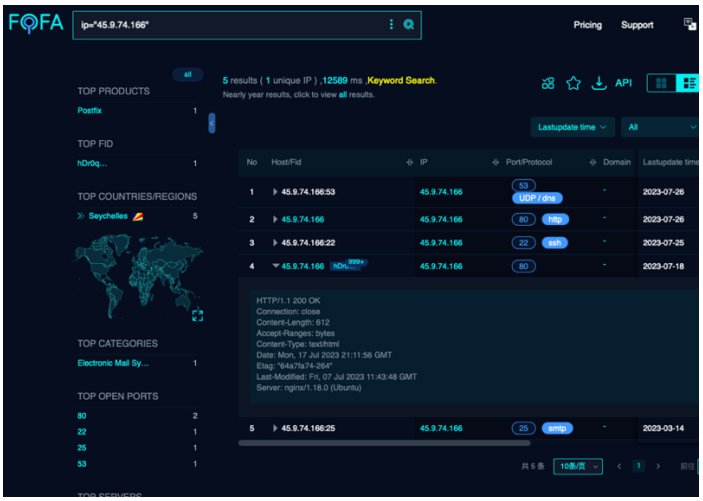


C2:

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

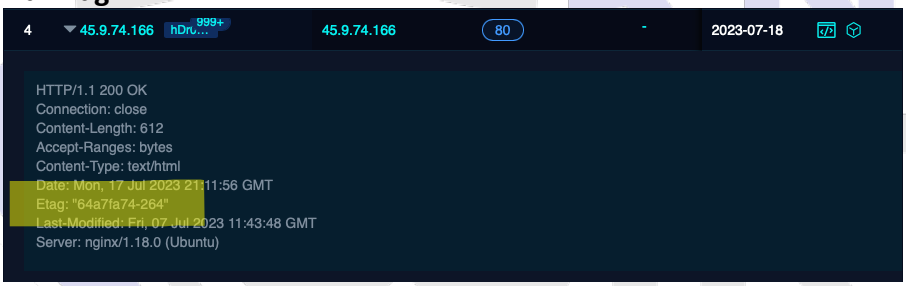
a) 45.9.74[.]166

Fofa.info:



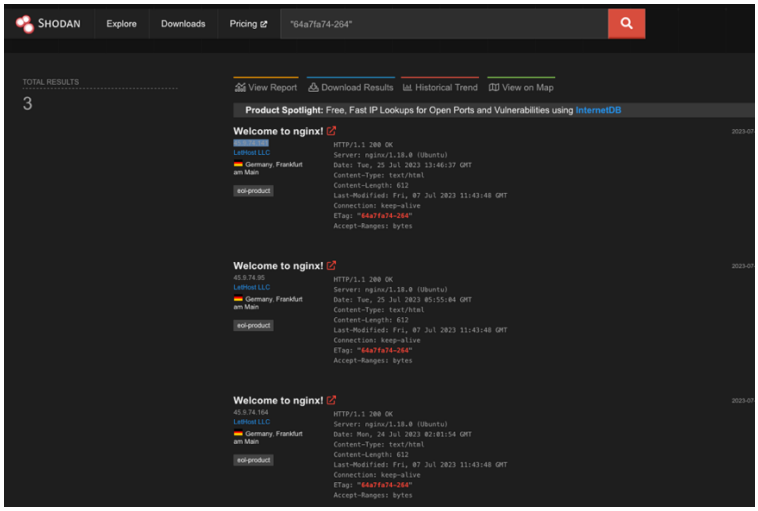
Szczegóły adresu IP serwera, z których możemy się dowiedzieć o wartości Etag: **"64a7fa74-264"**

Analiza ETag:

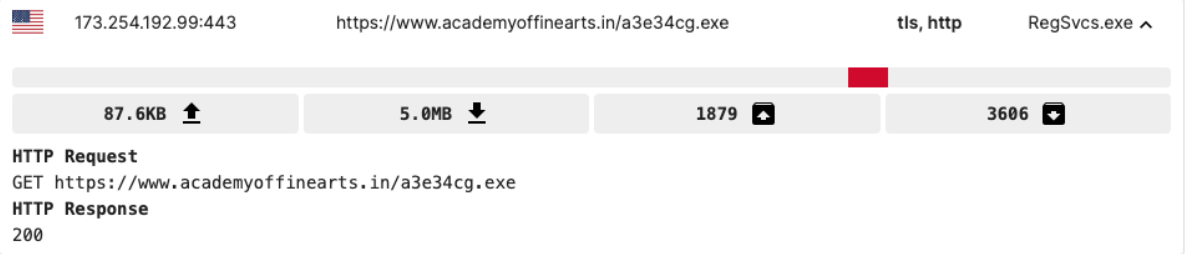


Sprawdzenie wartości Etag w narzędziu Shodan.io, skąd możemy się dowiedzieć o kolejnych dwóch adresach IP (adres .141 był już znany podczas analizy malware w tria.ge):

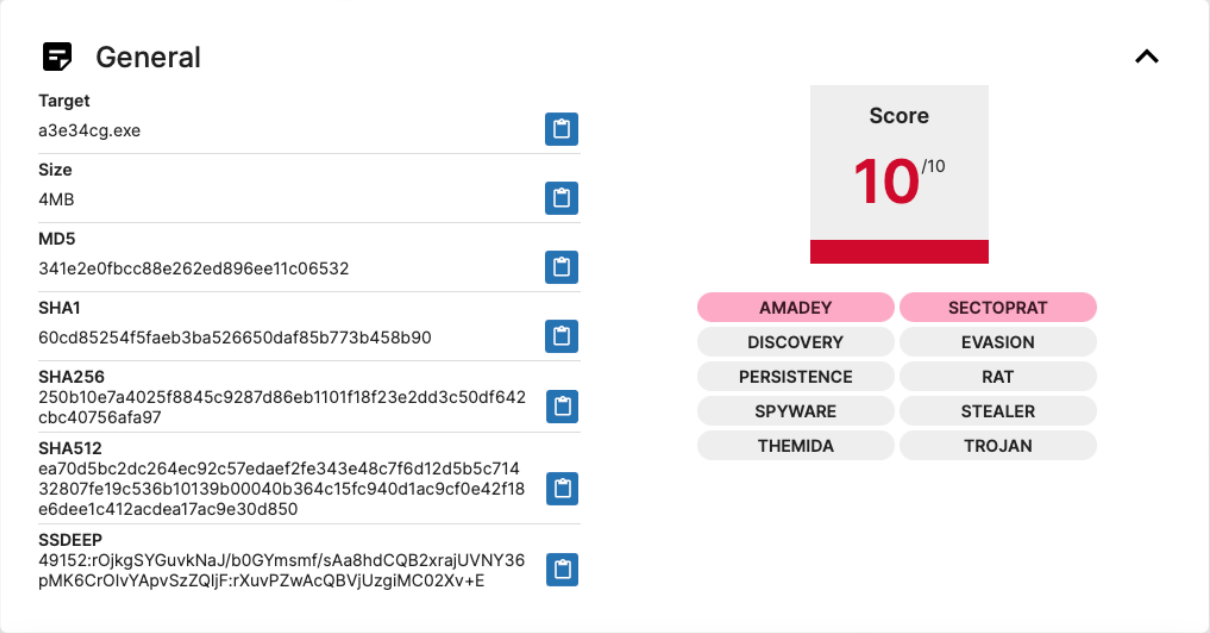
- 45.9.74.141 (https://www.virustotal.com/gui/ip-address/45.9.74.141);
- 45.9.74.95 (https://www.virustotal.com/gui/ip-address/45.9.74.95);
- 45.9.74.164 (https://www.virustotal.com/gui/ip-address/45.9.74.164);



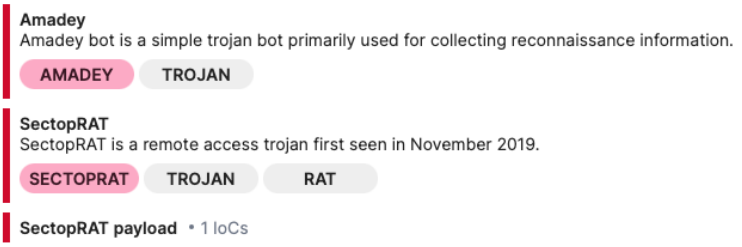
10) Pobranie kolejnego pliku .exe z adresu z którym, kontaktował się malware:



11) Analiza pliku: a3e34cg.exe w Tria.ge
(cały raport: https://tria.ge/230726-m6pfasba29/behavioral1):



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



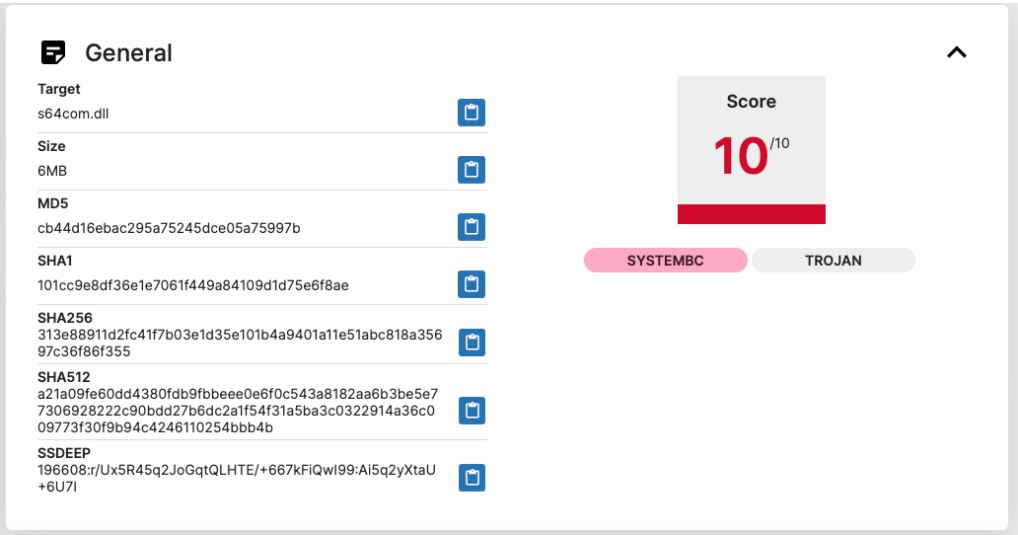
13) **Tak samo jak podczas analizy pierwszej próbki, sprawdzimy z jakimi IP łączy się złośliwe oprogramowanie:**

🇩🇪	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:

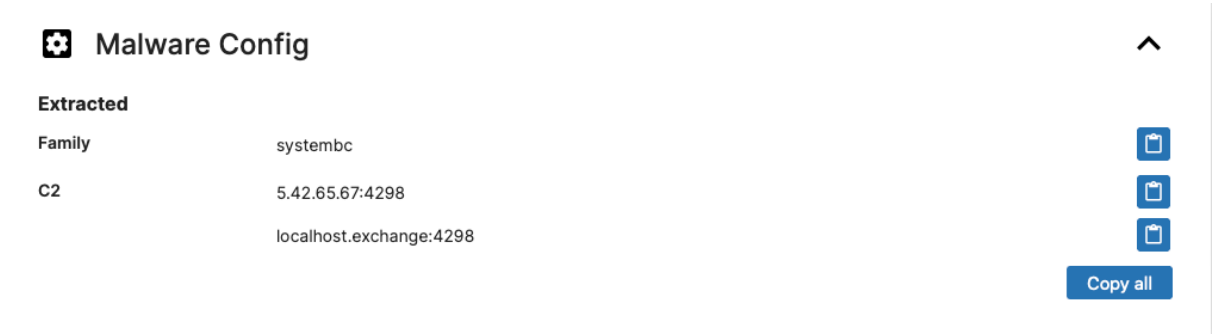
45.9.74.166:80
45.9.74.141:80
104.21.59.74:80
139.99.165.151:80
95.143.190.57:15647
5.42.65.67:4298 **– NOWY ADRES**

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)

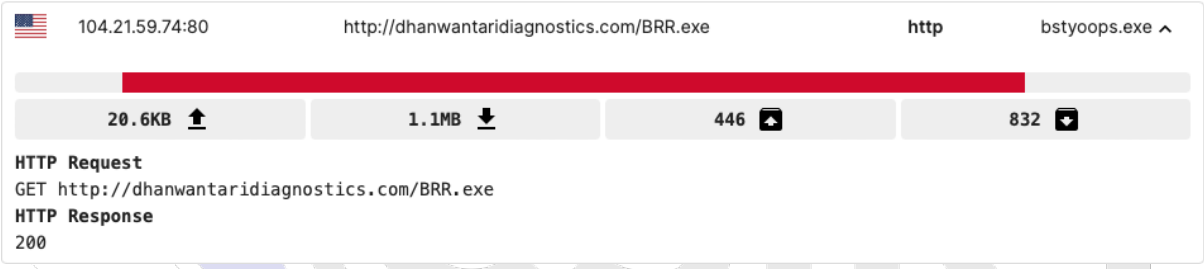


15) **Analiza wykazała, że w pliku s64com.dll zaszyte jest złośliwe oprogramowanie – SystemBC.**

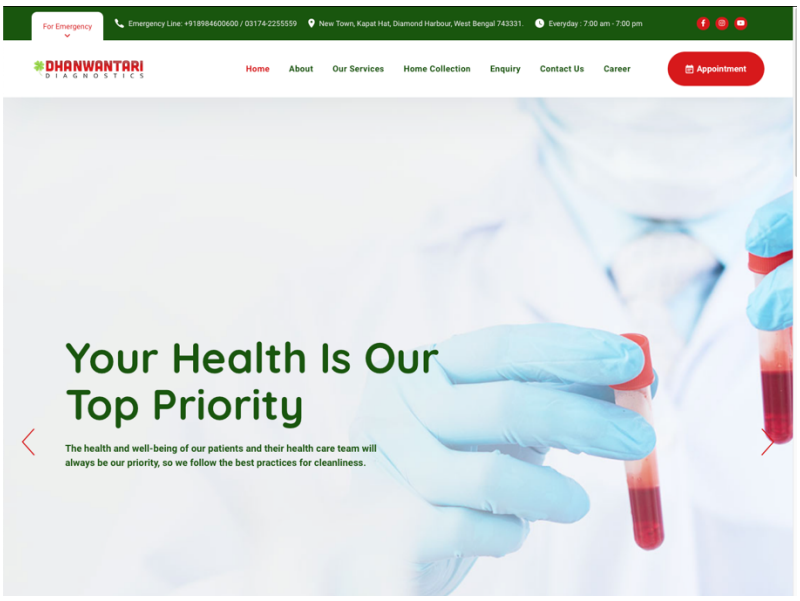
Adres IP: 5.42.65[.]67:4298 został już przez nas poznany w trakcie analizy poprzedniej próbki: a3e34cg.exe (https://www.virustotal.com/gui/ip-address/5.42.65.67/relations).



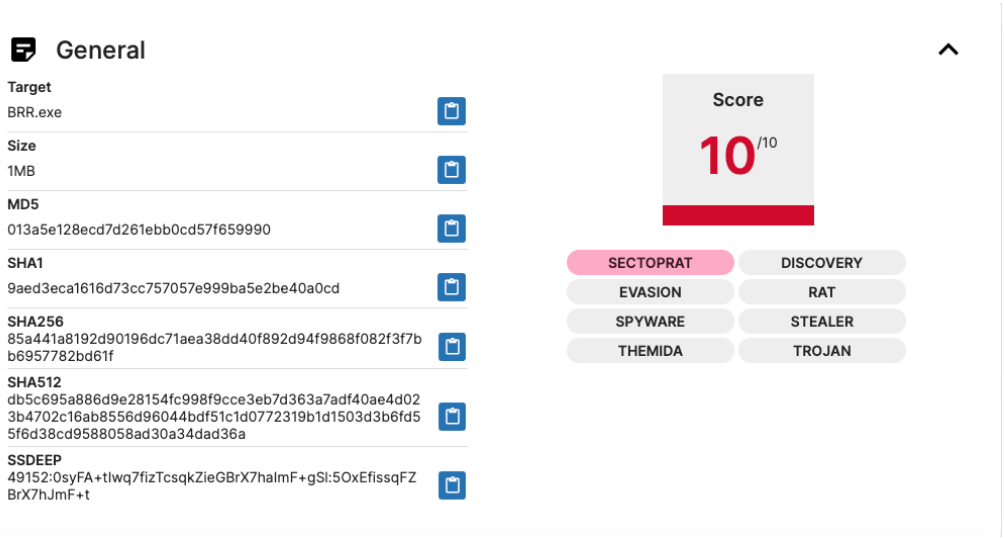
16) **Kolejną próbką, która została przeanalizowana i pochodzi z tej samej kampanii jest plik: BRR.exe, hostowany na:** hxxp://dhanwantaridiagnostics[.]com/BRR.exe



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



17) Analiza plikuBRR.exe w Tria.ge
(cały raport: https://tria.ge/230726-nx5xcsbb65/behavioral1):



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

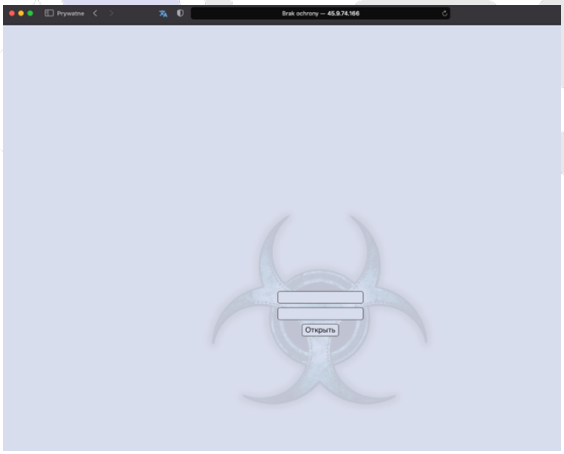
Ten raport z analizy złośliwego oprogramowania dostarcza szczegółowe informacje na temat działalności cyberprzestępczej prowadzonej na platformie YouTube. Szczególnie skupia się na metodzie dystrybucji złośliwego oprogramowania, polegającej na umieszczaniu linków do pobrania w opisach filmów.

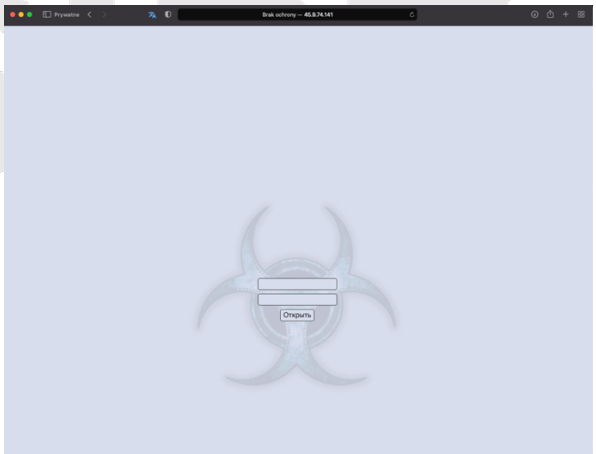
Badanie obejmowało pobieranie i analizę plików, które okazały się zawierać różne rodzaje złośliwego oprogramowania, w tym takie, które skupiają się na kradzieży informacji z urządzenia ofiary.

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.

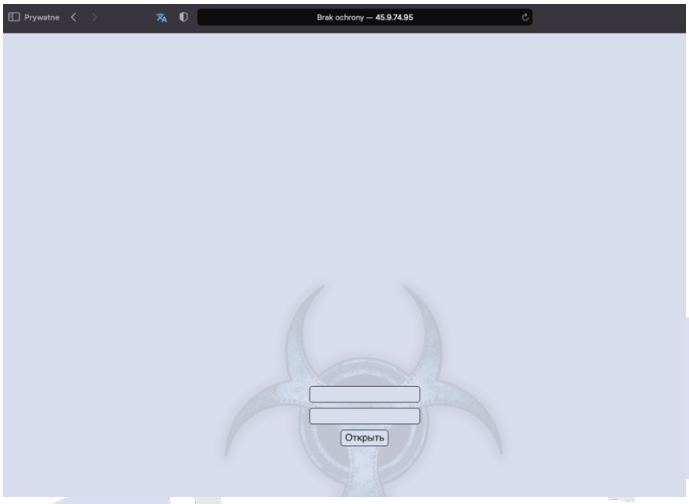
Są to adresy:
hxxp://45.9.74[.]141/b7djSDcPcZ/index.php
hxxp://45.9.74[.]166/b7djSDcPcZ/index.php

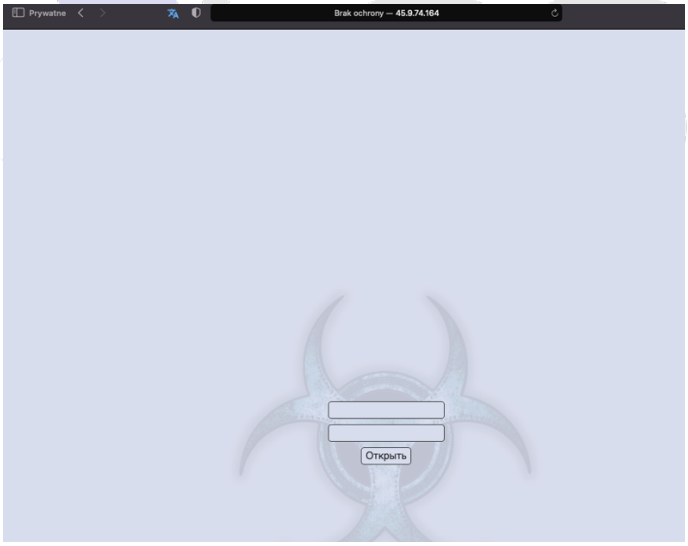
Pod ww. adresami możemy znaleźć panel logowania do AmadeyBot:





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`