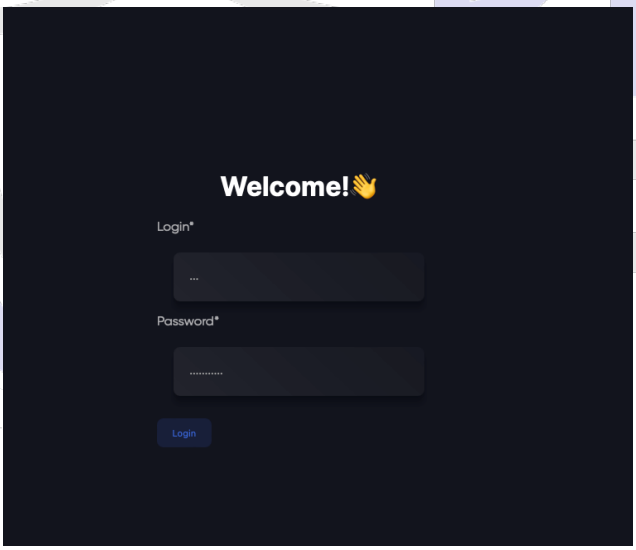
# AMOS/ATOMIC Stealer – malware na MAC OS

## Opis analizy:

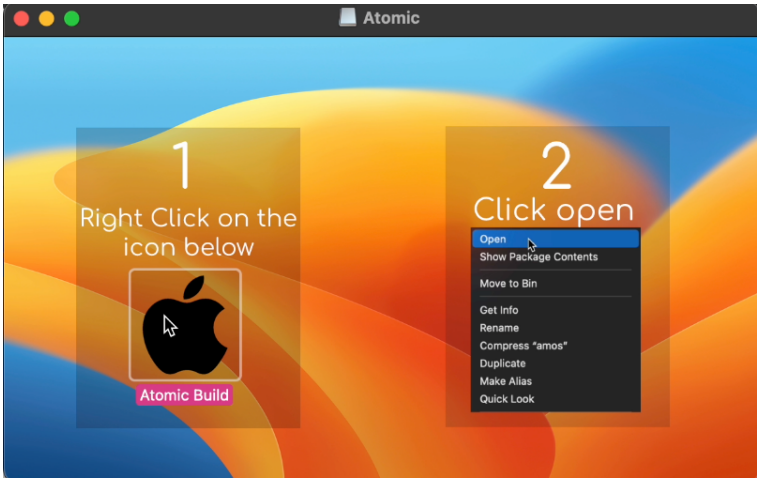
Stealer AMOS to specyficzny rodzaj oprogramowania złośliwego, który celuje w użytkowników korzystających z komputerów Mac. Jest to szczególnie niepokojące, gdyż przez lata systemy MAC OS były postrzegane jako stosunkowo odporne na ataki wirusów i malware. Stealer AMOS zmienia tę perspektywę, demonstrując, że żaden system nie jest całkowicie odporny na zagrożenia.

Co gorsza, przestępcy zdają się wykorzystywać bardziej wyrafinowane metody dystrybucji tego złośliwego oprogramowania. Poprzez umieszczanie reklam na platformach Google, docierają do szerszej publiczności, często nieświadomej ryzyka. To podejście sprawia, że Stealer AMOS może infekować komputery na niespotykaną dotąd skalę.

W niniejszym raporcie przeanalizujemy funkcjonowanie Stealera AMOS, sposoby jego dystrybucji oraz potencjalne metody obrony przed tym groźnym oprogramowaniem. Zrozumienie mechanizmów działania tego stealera jest kluczowe dla opracowania skutecznych strategii obrony i ochrony prywatności oraz danych użytkowników systemu MAC OS.




*Rysunek 1 Panel logowania do Stealer'a AMOS*




*Rysunek 2 Okno uruchomienia aplikacji, gdzie został zaszyty infostealer AMOS*

Problem z Stealerem AMOS nie ogranicza się jedynie do jego działania. Sytuację komplikuje fakt, że przestępcy opublikowali instrukcje, jak korzystać z tego złośliwego narzędzia. Dostarczenie takich informacji może ułatwić innym złodziejom danych dostęp do narzędzi i technik, które wcześniej były może mniej dostępne. To wyraźnie pokazuje, że zagrożenie nie jest statyczne i że środki obronne muszą się rozwijać równie dynamicznie jak strategie przestępców.

## Atomic Stealer - Logo overview

Atomic Dev. • June 27, 2023

Good day, dear readers. In this article, I will describe the structure of the Atomic Stealer log. When creating the stiller, we tried to stick to the general picture of the log types, but made some changes, which I will now talk about

> *https://t.me/amos_macos*
> *https://t.me/amos_macos*
> *https://t.me/amos_macos*

**General view of the log:**

| | |
|---|---|
| US.108.213.30.76 | Folder |
| Passwords.txt | Plain Text Document |
| Autofills.txt | Plain Text Document |
| UserInformation.txt | Plain Text Document |
| FileGrabber | Folder |
| Wallets | Folder |
| Cookies | Folder |
| keychain.txt | Plain Text Document |

Log - Atomic Stealer

*UserInformation.txt*

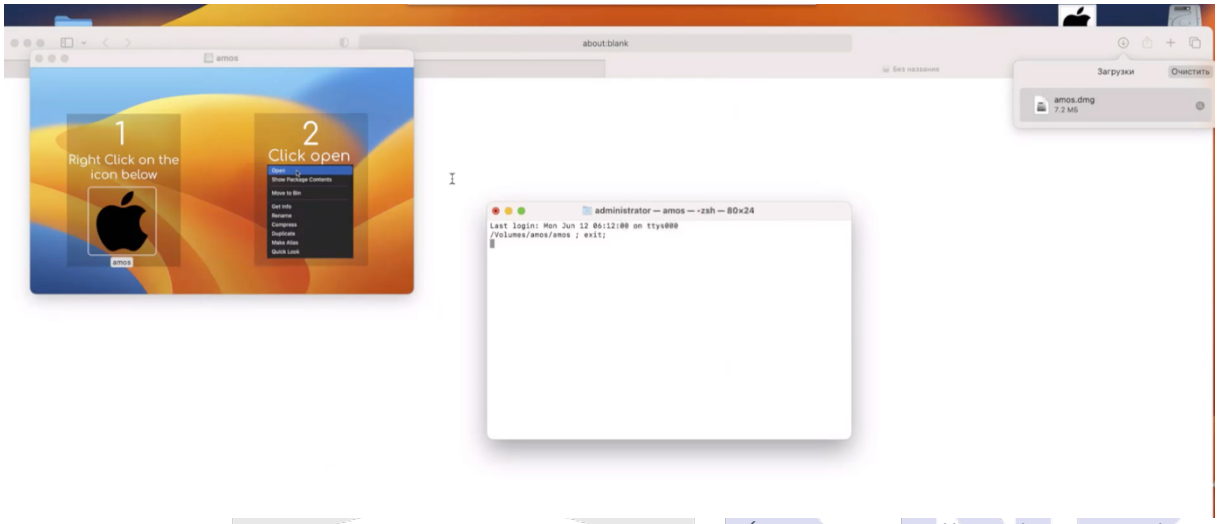
> *A text file containing information about the victim.*

```
ATOMIC MAC STEALER V1.1

MetaMask Info:
Seeds: british lock dock pock tong back exercise emotion priority teach please crumble
Private Keys: Atomic000000
Debanks: https://debank.com/profile/0x45d110bc7f3be56c01bc11c4fb5da07a9bb9b373
https://debank.com/profile/0x457f88887ebd88c1a0463bd322b60792ac102c4e


Userinfo:
Country: US
IP: 108.43.28.31
City: Boulder
Hardware:

    Hardware Overview:

      Model Name: MacBook Air
      Model Identifier: MacBookAir9,1
      Processor Name: Quad-Core Intel Core i7
      Processor Speed: 1.2 GHz
      Number of Processors: 1
      Total Number of Cores: 4
      L2 Cache (per Core): 512 KB
      L3 Cache: 8 MB
      Hyper-Threading Technology: Enabled
      Memory: 16 GB
      System Firmware Version: 1968.120.12.0.0 (iBridge: 20.16.5058.0.0,0)
      OS Loader Version: 577~170
      Serial Number (system): C02CT0NYMLVD
      Hardware UUID: 5D99D4BC-1EAA-50EA-955A-3F8ABD1504ED
      Provisioning UDID: 5D99D4BC-1EAA-50EA-955A-3F8ABD1504ED
      Activation Lock Status: Disabled
```

UserInformation.txt - Atomic Stealer

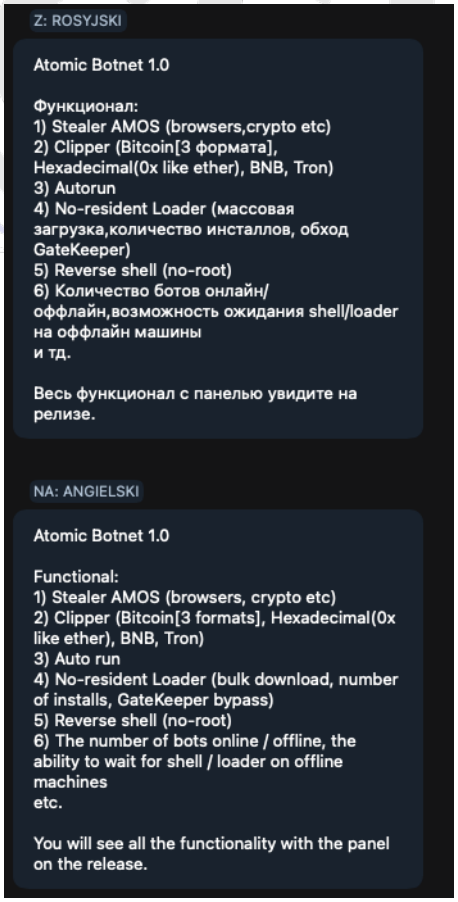
*Rysunek 3 Instrukcja Atomic/AMOS Stealera*

Stealer AMOS wykorzystuje specjalnie spreparowane instalatory o rozszerzeniu .dmg, które jest domyślnym typem pliku obrazu dysku dla systemu MAC OS. Użytkownicy, nieświadomi zagrożenia, mogą pobrać i uruchomić te pozornie niegroźne pliki, nie zdając sobie sprawy, że w instalatorze jest zaszyte złośliwe oprogramowanie Amos Stealer.

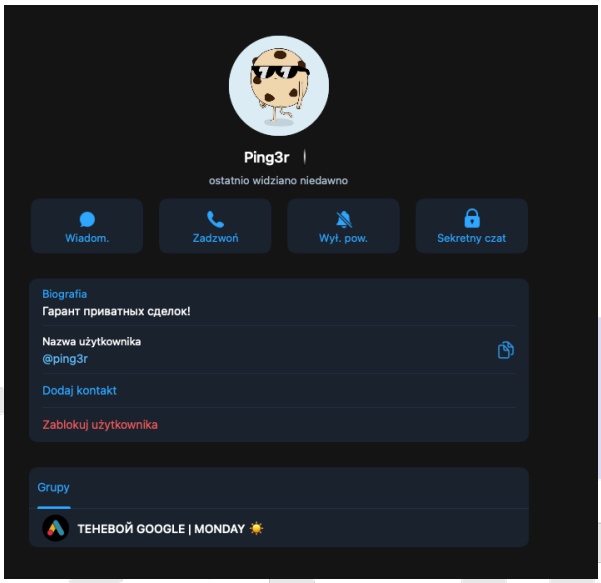



*Rysunek 4 Film prezentujący plik .dmg mający zaszytego AMOS Stealera. Źródło filmu: hxxps://t[.]me/amos_macos/36*

**Funkcjonalność AMOS Stealer'a (pisownia oryginalna):**



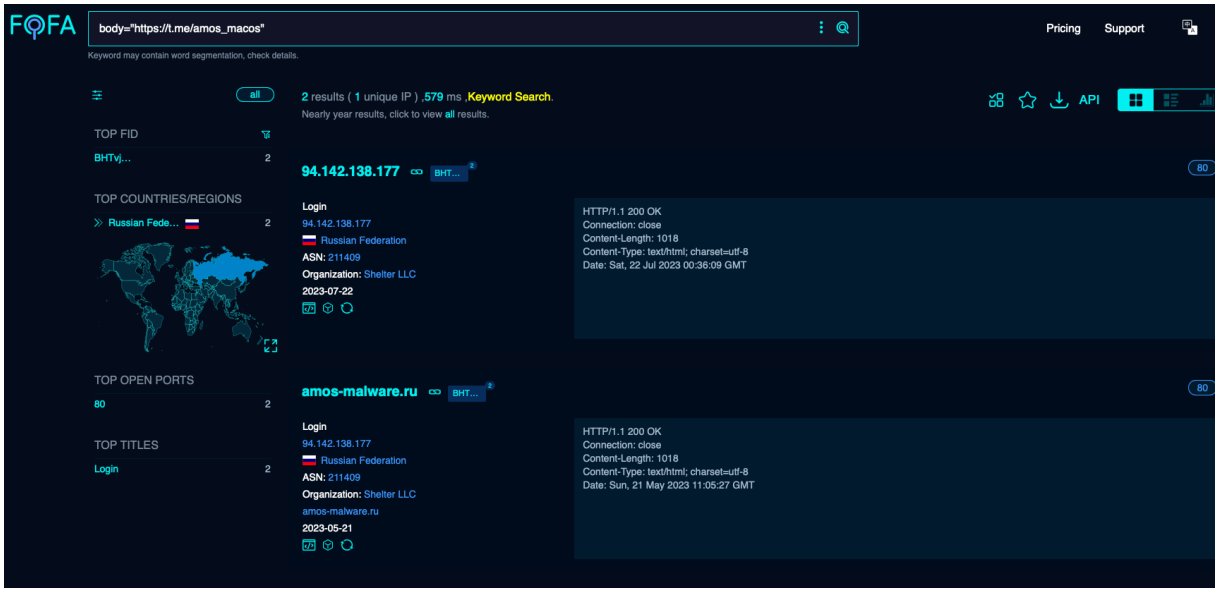
Podczas szczegółowej analizy na platformie Telegram, zidentyfikowaliśmy, że admin, będący właścicielem Stealera AMOS, jest również użytkownikiem grupy zajmującej się kupowaniem kont reklamowych Google oraz dystrybucją fałszywych reklam. To odkrycie może wskazywać na większą, zorganizowaną sieć przestępczą, w której uczestnicy współpracują, by promować i rozpowszechniać różne rodzaje złośliwego oprogramowania, w tym stealerów. Ta informacja podkreśla wagę stałego monitorowania i analizy aktywności online, aby zrozumieć, jak działają takie sieci i jak można przeciwdziałać ich nielegalnym praktykom.




*Rysunek 5 Konto właściciela AMOS Stealer'a w komunikatorze Telegram*

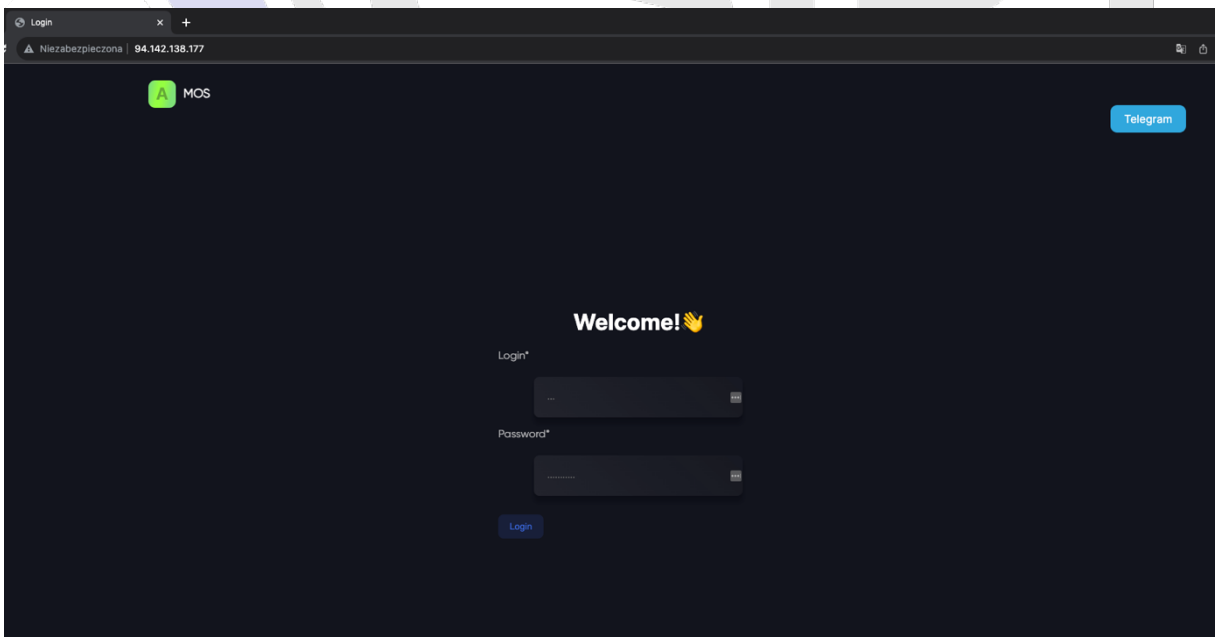
Po zidentyfikowaniu konta admina Amos stealera, wykorzystaliśmy serwis fofa.info do przeprowadzenia konkretnej analizy.
Używając zapytania **body="https://t.me/amos_macos"**, udało nam się zlokalizować panel logowania do stealera.


*Rysunek 6 - konto w komunikatorze Telegram, odpowiedzialne za kontakt z kupującymi*



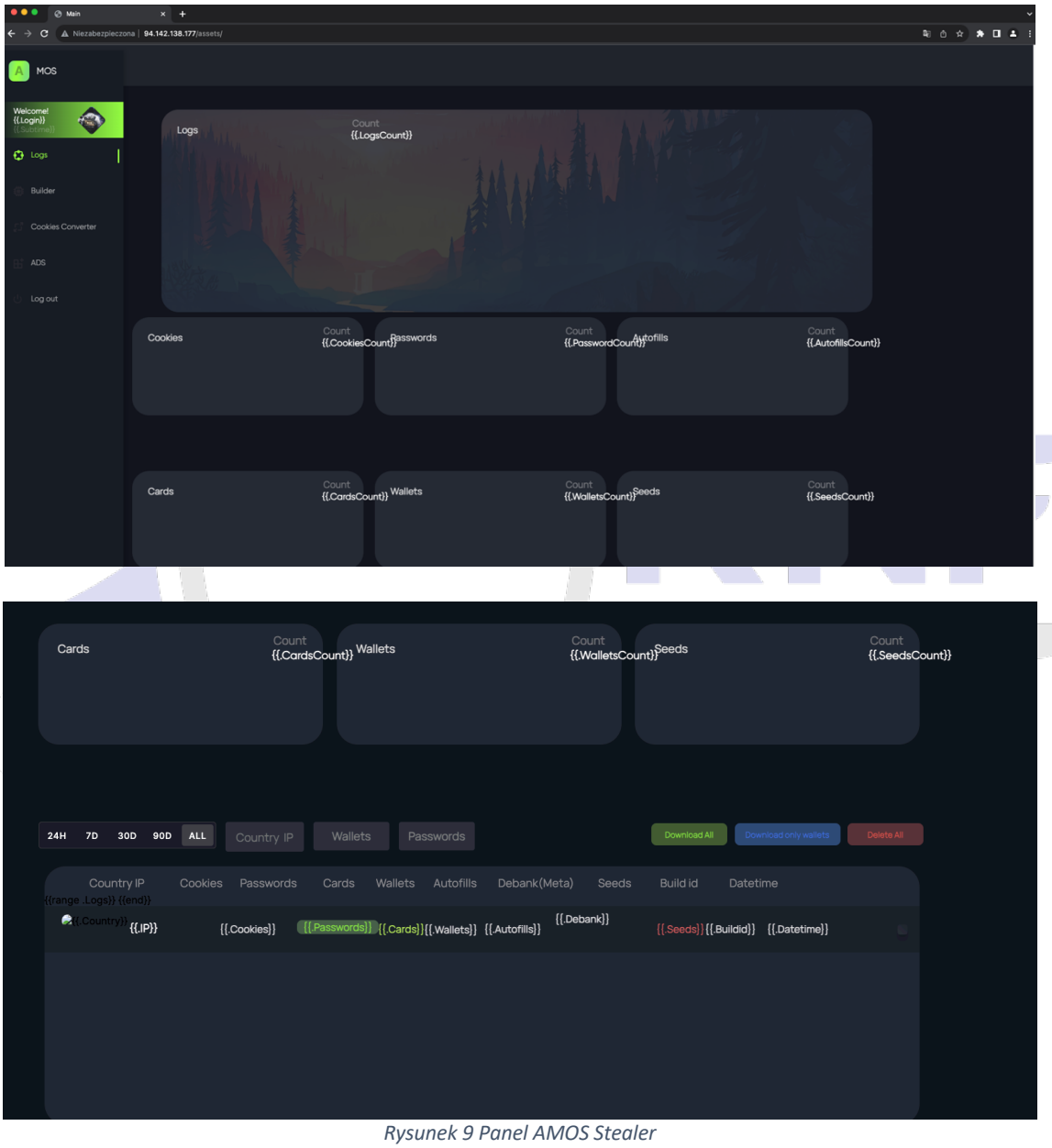

*Rysunek 7 Query w serwisie FOFA.info: body="https://t.me/amos_macos"*

Dzięki temu odkryciu, udało nam się zlokalizować logowanie do panelu stealera, dostępne pod adresem IP 94.142.138[.]177. To konkretne znalezisko dostarcza nam bezpośredniego dostępu do obszaru, w którym przestępcy mogą zarządzać swoim złośliwym oprogramowaniem, dając nam unikalny wgląd w ich działalność oraz potencjalne ścieżki do dalszej analizy.




*Rysunek 8 Panel logowania do AMOS Stealera*

Podczas fuzzowania powyższego adresu IP zlokalizowaliśmy konkretny adres URL: **http://94.142.138[.]177/assets/**. Odwiedzając ten adres, możemy zobaczyć bezpośredni wygląd panelu stealera.

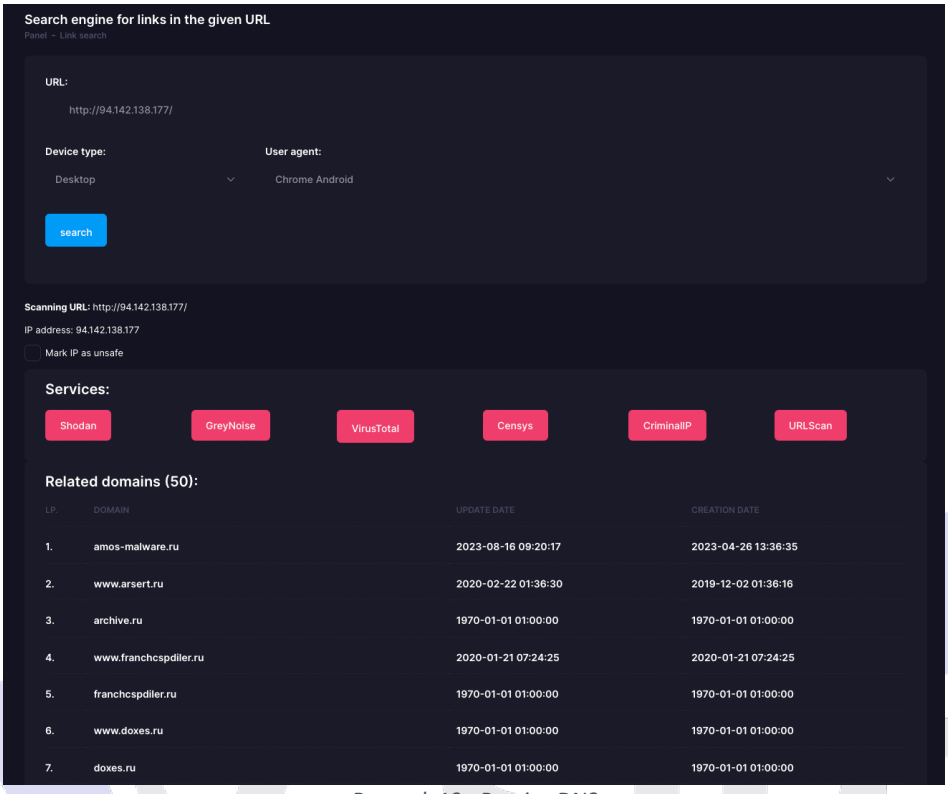




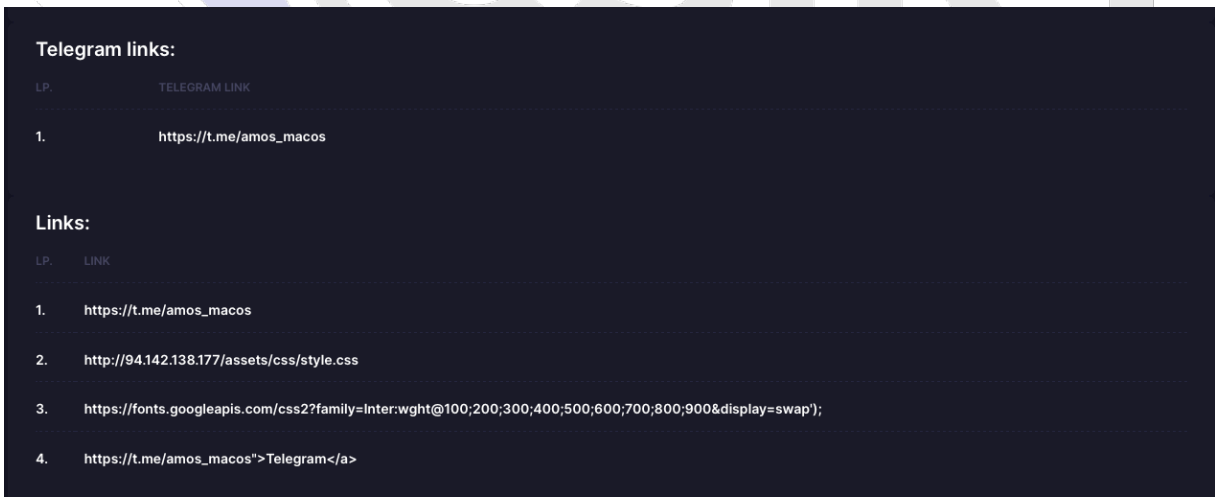


*Rysunek 9 Panel AMOS Stealer*

## Analiza URL prowadzącego do panelu AMOS Stealer wraz z Passive DNS:




*Rysunek 10 - Passive DNS*




*Rysunek 11 Linki zaszyte na stronie panelu.*

**Jak chronić się przed złośliwym oprogramowaniem takim jak stealer AMOS?**

Chronienie się przed stealermi, takimi jak Amos stealer, nie musi być skomplikowane. Oto kilka prostych kroków, które można podjąć, aby zminimalizować ryzyko:

1. **Pobieranie Aplikacji z Zaufanych Źródeł**: Należy pobierać aplikacje i oprogramowanie wyłącznie z zaufanych źródeł, takich jak Apple Store. Unikając nieznanych i niezweryfikowanych stron, znacznie zmniejszasz ryzyko zainfekowania systemu złośliwym oprogramowaniem.
2. **Aktualizacja Oprogramowania**: Regularne aktualizowanie systemu operacyjnego i zainstalowanego oprogramowania zapewnia, że korzystasz z najnowszych zabezpieczeń i łatek, które mogą zapobiec infekcji stealermi.
3. **Ostrożność przy Klikaniu**: Zachowanie ostrożności przy klikaniu na linki i pobieraniu załączników, zwłaszcza od nieznanych źródeł, jest kluczowe.
4. **Edukacja i Świadomość**: Bycie świadomym typowych metod, jakimi posługują się przestępcy (np. fałszywe reklamy, phishing), oraz edukacja na temat bezpiecznego korzystania z internetu, może prowadzić do bardziej ostrożnego i świadomego korzystania z sieci.