AMOS/ATOMIC Stealer - malware on MAC OS.

Analysis description:

The AMOS stealer is a specific type of malware that targets Mac users. This is particularly worrisome because for years MAC OS systems have been seen as relatively immune to virus and malware attacks. The AMOS stealer changes that perspective, demonstrating that no system is completely immune to threats.

To make matters worse, criminals seem to be using more sophisticated methods to distribute this malware. By placing ads on Google platforms, they are reaching a wider audience, often unaware of the risks. This approach allows Stealer AMOS to infect computers on an unprecedented scale.

In this report, we will analyze how the AMOS Stealer works, how it is distributed, and potential methods of defense against this menacing software. Understanding the mechanisms of this stealer is crucial to developing effective strategies to defend and protect the privacy and data of MAC OS users.

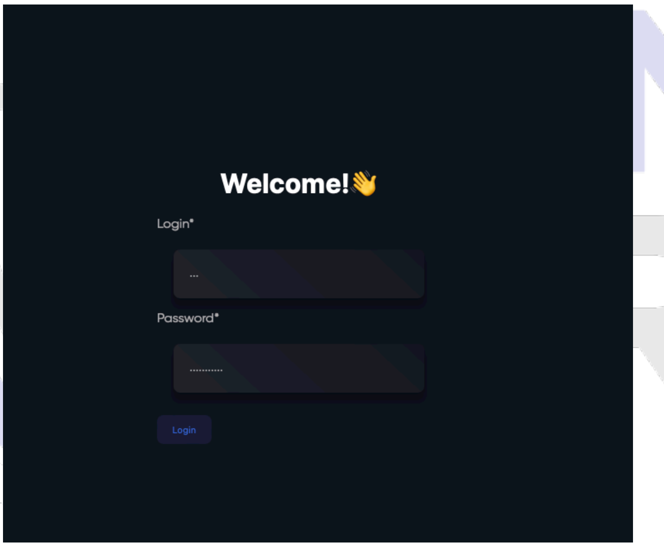
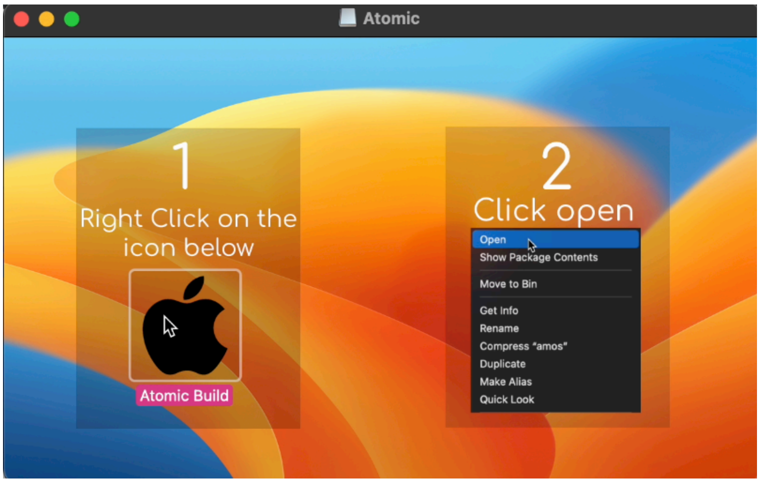


Figure 1 AMOS Stealer login panel

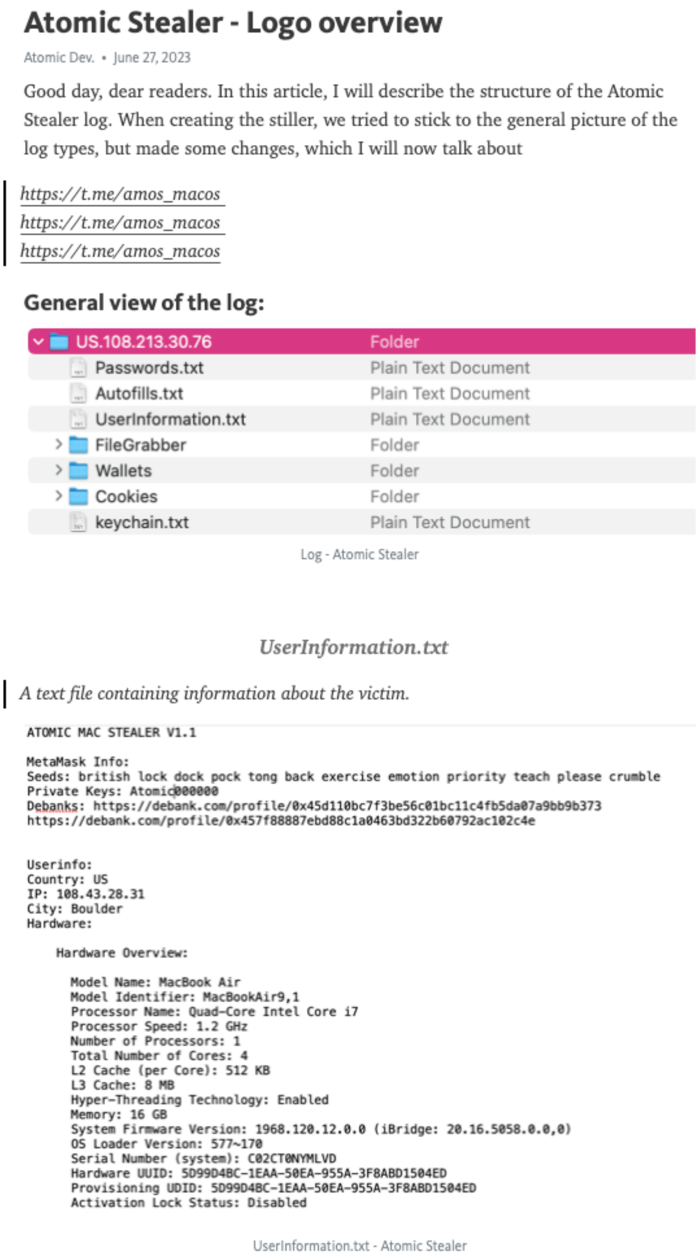


1 Right Click on the icon below

2 Click open

Figure 2 The application launch window, where the AMOS infostealer has been sewn in

The problem with the AMOS Stealer is not limited to its operation. The situation is complicated by the fact that criminals have published instructions on how to use this malicious tool. Providing such information can make it easier for other data thieves to access tools and techniques that were perhaps less accessible before. This clearly shows that the threat is not static and that defensive measures must evolve as dynamically as the criminals' strategies.



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

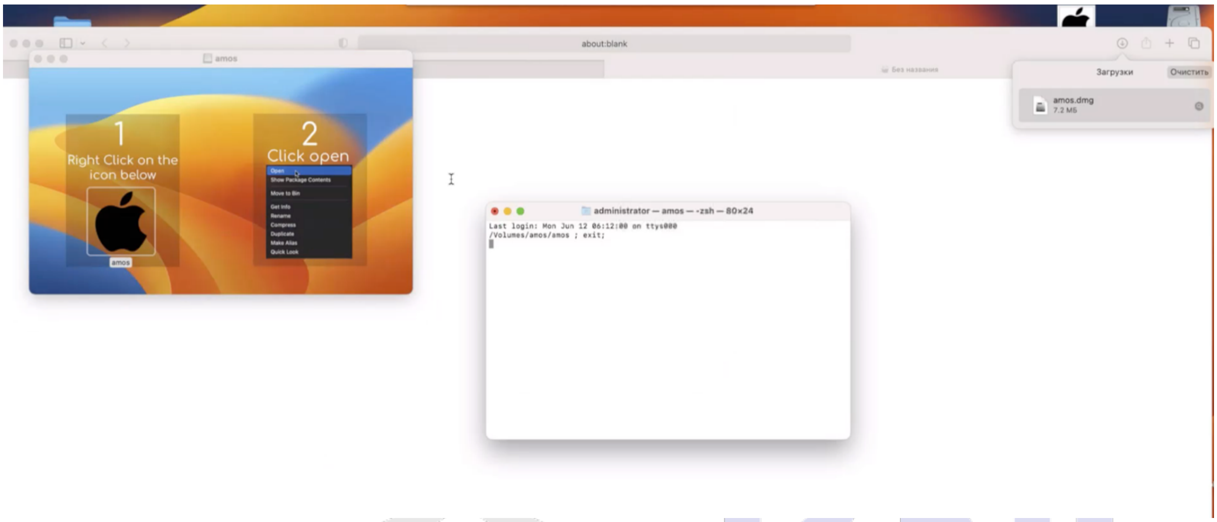
> *A text file containing information about the victim.*

```
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

Figure 3 Atomic/AMOS Stealer manual

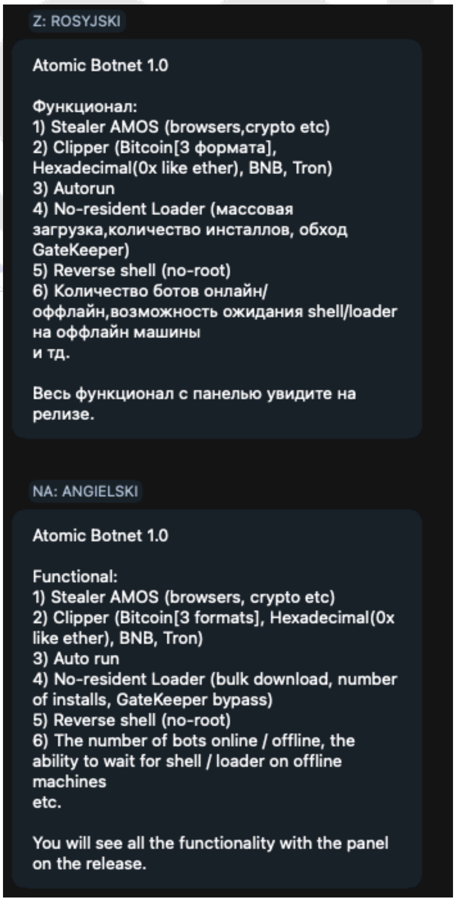
AMOS Stealer uses specially crafted installers with a .dmg extension, which is the default disk image file type for MAC OS. Users, unaware of the threat, may download and run these seemingly harmless files without realizing that Amos Stealer malware is sewn into the installer.



```
Last login: Mon Jun 12 06:12:00 on ttys000
/Volumes/amos/amos ; exit;
```

Figure 4 A video showing a .dmg file that has AMOS Stealer sewn into it. Video source: hxxps://t[.]me/amos_macos/36

AMOS Stealer's functionality (original spelling):


Z: ROSYJSKI

Atomic Botnet 1.0

Функционал:
1) Stealer AMOS (browsers,crypto etc)
2) Clipper (Bitcoin[3 формата], Hexadecimal(0x like ether), BNB, Tron)
3) Autorun
4) No-resident Loader (массовая загрузка,количество инсталлов, обход GateKeeper)
5) Reverse shell (no-root)
6) Количество ботов онлайн/оффлайн,возможность ожидания shell/loader на оффлайн машины
и тд.

Весь функционал с панелью увидите на релизе.

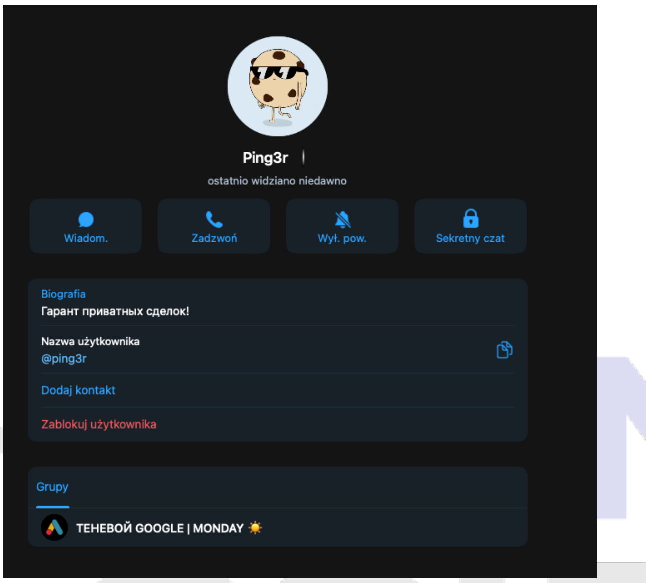
NA: ANGIELSKI

Atomic Botnet 1.0

Functional:
1) Stealer AMOS (browsers, crypto etc)
2) Clipper (Bitcoin[3 formats], Hexadecimal(0x like ether), BNB, Tron)
3) Auto run
4) No-resident Loader (bulk download, number of installs, GateKeeper bypass)
5) Reverse shell (no-root)
6) The number of bots online / offline, the ability to wait for shell / loader on offline machines
etc.

You will see all the functionality with the panel on the release.

During a detailed analysis on the Telegram platform, we identified that the admin who owns the AMOS stealer is also a user of a group involved in buying Google ad accounts and distributing fake ads. This discovery may be indicative of a larger, organized criminal network in which participants work together to promote and distribute various types of malware, including stealers. This news underscores the importance of constantly monitoring and analyzing online activity to understand how such networks operate and how their illegal practices can be countered.



Ping3r

ostatnio widziano niedawno

Biografia
Гарант приватных сделок!

Nazwa użytkownika
@ping3r

Dodaj kontakt

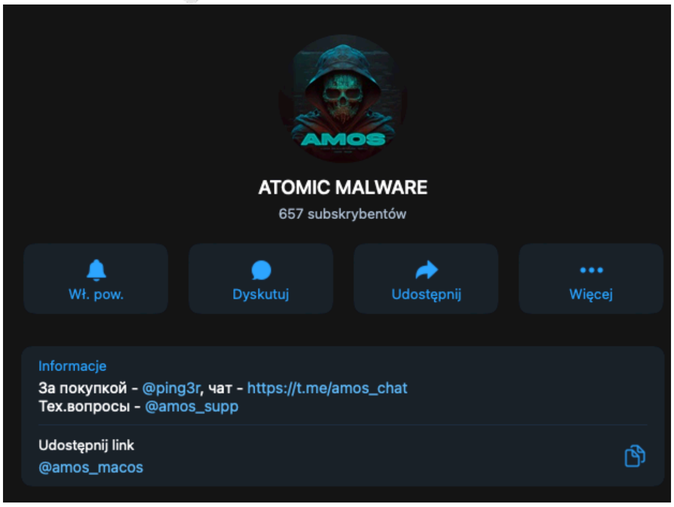
Zablokuj użytkownika

Grupy

ТЕНЕВОЙ GOOGLE | MONDAY ☀️

Figure 5 AMOS Stealer owner's account in Telegram messenger

After identifying the Amos stealer admin account, we used fofa.info to conduct a specific analysis.
Using the query **body="https://t.me/amos_macos"**, we were able to locate the login panel for the stealer.



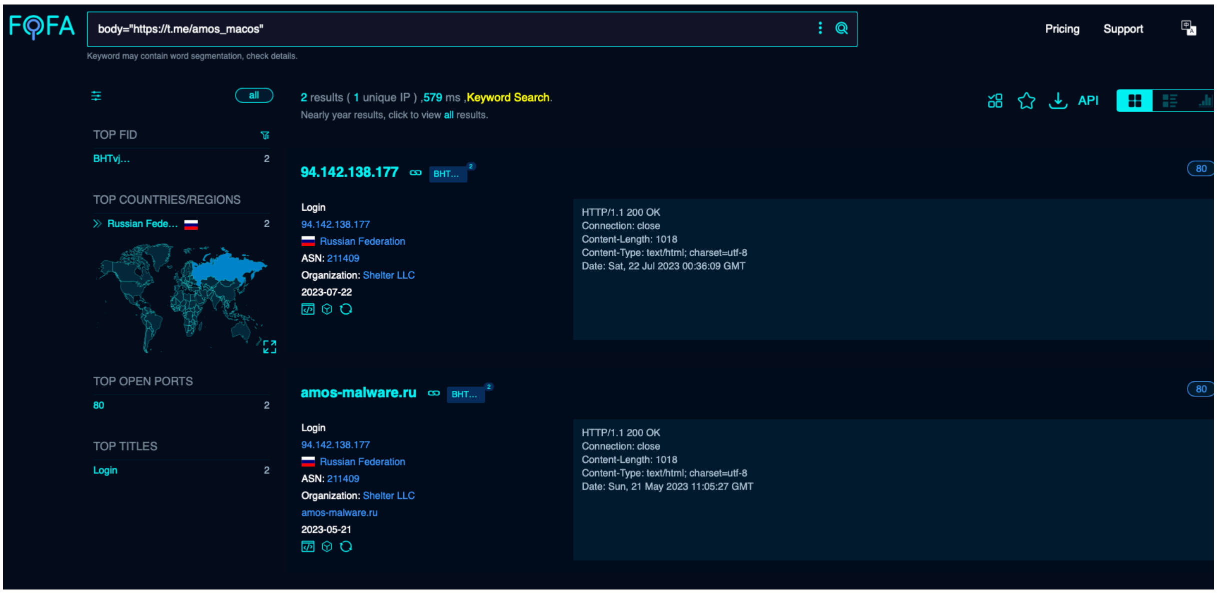
ATOMIC MALWARE

657 subskrybentów

Informacje
За покупкой - @ping3r, чат - https://t.me/amos_chat
Тех.вопросы - @amos_supp

Udostępnij link
@amos_macos

Figure 6 - Telegram messenger account, responsible for contacting buyers



body="https://t.me/amos_macos"

Keyword may contain word segmentation, check details.

2 results (1 unique IP) ,579 ms ,Keyword Search.
Nearly year results, click to view all results.

TOP FID	
BHTvj...	2

TOP COUNTRIES/REGIONS	
Russian Fede...	2

TOP OPEN PORTS	
80	2

TOP TITLES	
Login	2

94.142.138.177 BHT... 80

Login
94.142.138.177
Russian Federation
ASN: 211409
Organization: Shelter LLC
2023-07-22

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 1018
Content-Type: text/html; charset=utf-8
Date: Sat, 22 Jul 2023 00:36:09 GMT
```

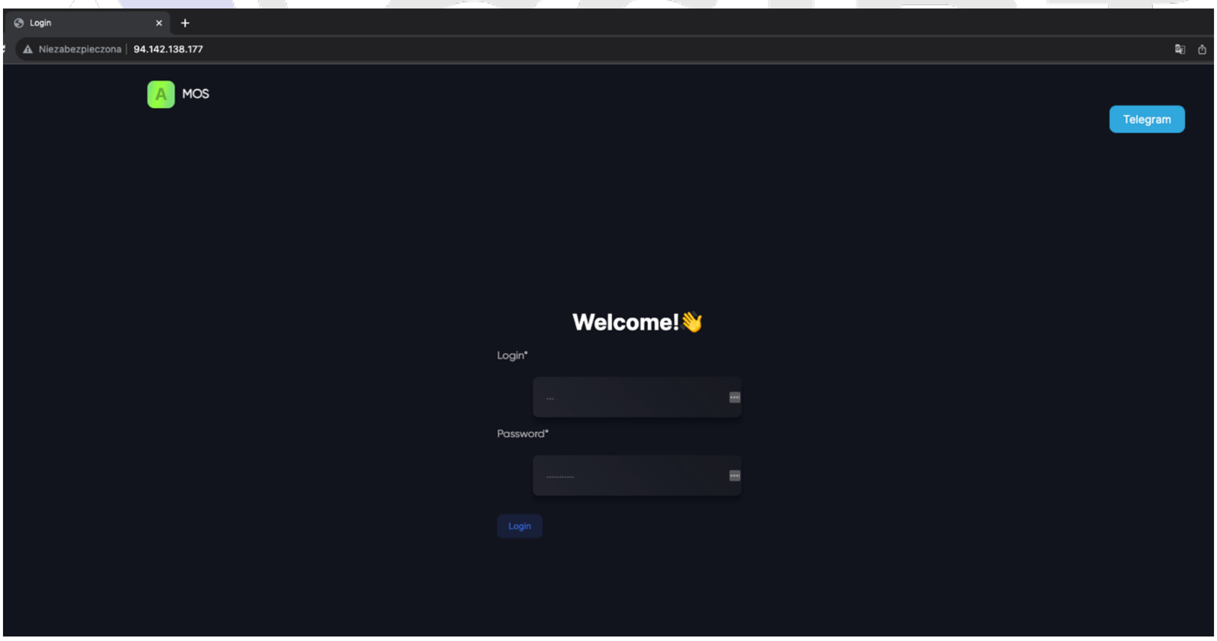
amos-malware.ru BHT... 80

Login
94.142.138.177
Russian Federation
ASN: 211409
Organization: Shelter LLC
amos-malware.ru
2023-05-21

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 1018
Content-Type: text/html; charset=utf-8
Date: Sun, 21 May 2023 11:05:27 GMT
```

Figure 7 Query at FOFA.info: body="https://t.me/amos_macos"

With this discovery, we were able to locate the stealer's panel login, available at IP address 94.142.138[.]177. This particular find provides us with direct access to the area where criminals can manage their malware, giving us unique insight into their activities and potential paths for further analysis.



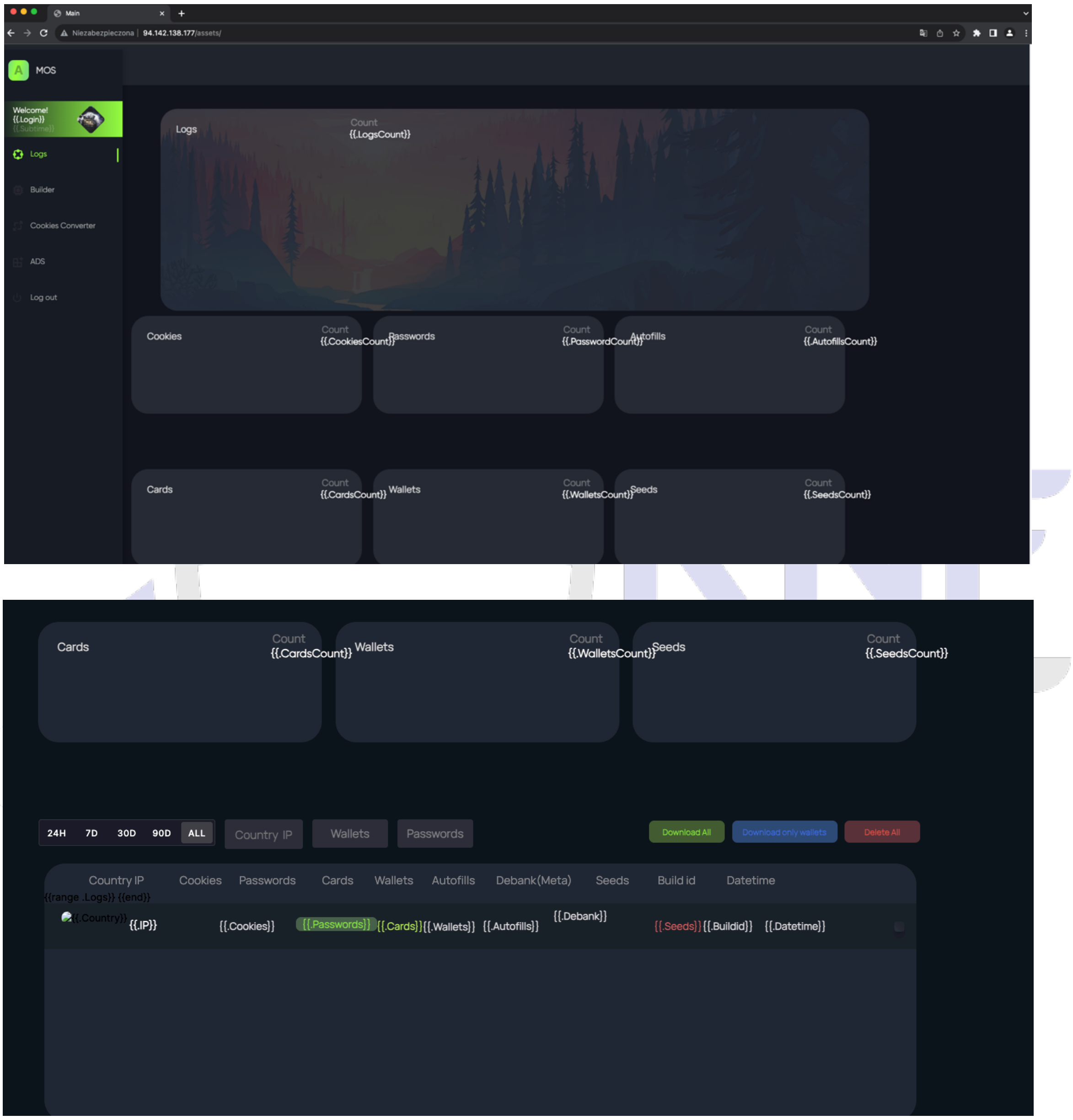
Welcome!👋

Login*

Password*

Figure 8 AMOS Stealer login panel

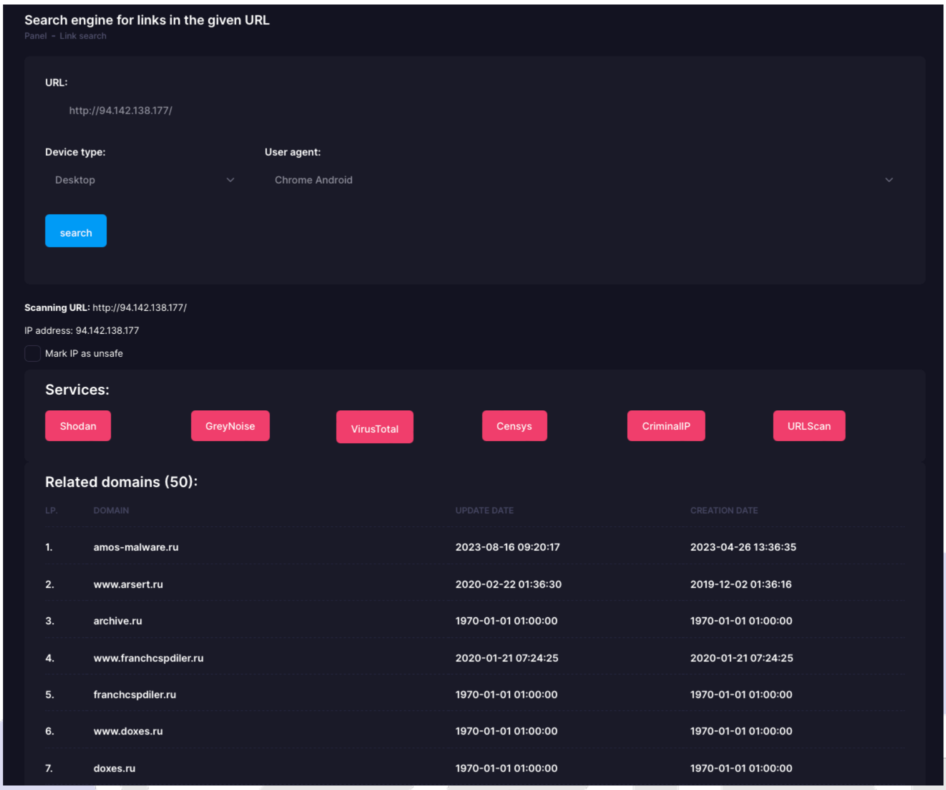
While fuzzing the above IP address, we located a specific URL: **http://94.142.138[.]177/assets/**. By visiting this address, we can see the direct appearance of the stealer panel.



Country IP	Cookies	Passwords	Cards	Wallets	Autofills	Debank(Meta)	Seeds	Build id	Datetime
{{range .Logs}} {{end}}									
{{.Country}} {{.IP}}	{{.Cookies}}	{{.Passwords}}	{{.Cards}}	{{.Wallets}}	{{.Autofills}}	{{.Debank}}	{{.Seeds}}	{{.Buildid}}	{{.Datetime}}

Figure 9 AMOS Stealer panel

Analysis of the URL leading to the AMOS Stealer panel along with Passive DNS:



Search engine for links in the given URL

URL: http://94.142.138.177/

Device type: Desktop

User agent: Chrome Android

Scanning URL: http://94.142.138.177/

IP address: 94.142.138.177

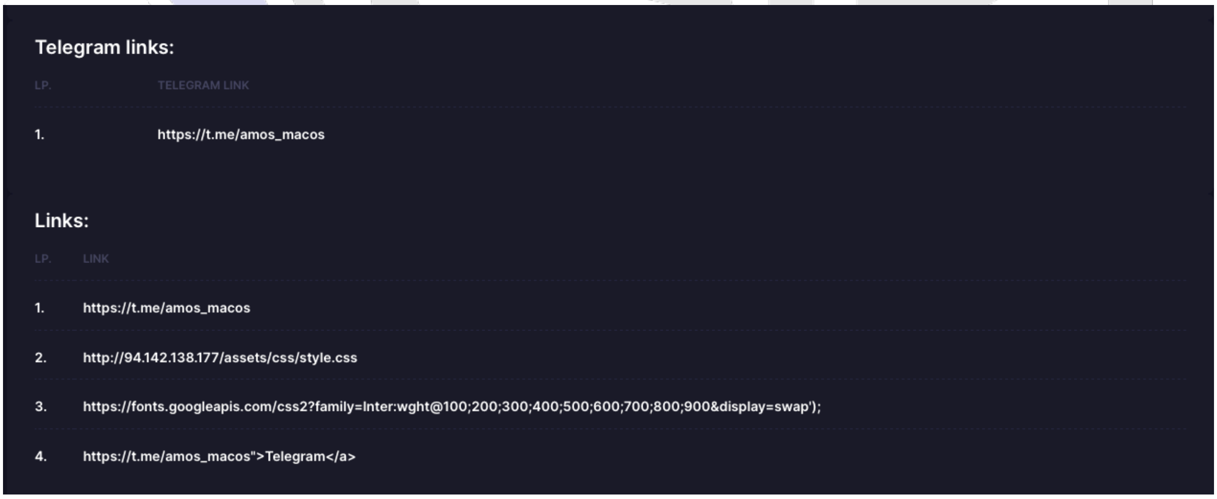
□ Mark IP as unsafe

Services:

Related domains (50):

LP.	DOMAIN	UPDATE DATE	CREATION DATE
1.	amos-malware.ru	2023-08-16 09:20:17	2023-04-26 13:36:35
2.	www.arsert.ru	2020-02-22 01:36:30	2019-12-02 01:36:16
3.	archive.ru	1970-01-01 01:00:00	1970-01-01 01:00:00
4.	www.franchcspdiler.ru	2020-01-21 07:24:25	2020-01-21 07:24:25
5.	franchcspdiler.ru	1970-01-01 01:00:00	1970-01-01 01:00:00
6.	www.doxes.ru	1970-01-01 01:00:00	1970-01-01 01:00:00
7.	doxes.ru	1970-01-01 01:00:00	1970-01-01 01:00:00

Figure 10 - Passive DNS



Telegram links:

LP.	TELEGRAM LINK
1.	https://t.me/amos_macos

Links:

LP.	LINK
1.	https://t.me/amos_macos
2.	http://94.142.138.177/assets/css/style.css
3.	https://fonts.googleapis.com/css2?family=Inter:wght@100;200;300;400;500;600;700;800;900&display=swap');
4.	https://t.me/amos_macos">Telegram</a>

Figure 11 Links sewn into the panel page.

How to protect yourself from malware such as AMOS stealer?

Protecting yourself from stealers such as Amos stealer doesn't have to be complicated. Here are some simple steps you can take to minimize your risk:

1. **Downloading Apps from Trusted Sources**: Only download apps and software from trusted sources, such as the Apple Store. By avoiding unknown and unverified sites, you greatly reduce the risk of infecting your system with malware.
2. **Software Updates**: Regularly updating your operating system and installed software ensures that you are using the latest security features and patches that can prevent stealermi infections.
3. **Caution When Clicking**: Exercising caution when clicking on links and downloading attachments, especially from unknown sources, is key.
4. **Education and Awareness**: Being aware of the typical methods criminals use (e.g., false advertising, phishing), and educating yourself on how to use the Internet safely, can lead to more cautious and informed online use.