FakeSG campaign, Akira ransomware and AMOS macOS stealer

securelist.com/crimeware-report-fakesg-akira-amos/111483/

Authors

GReAT

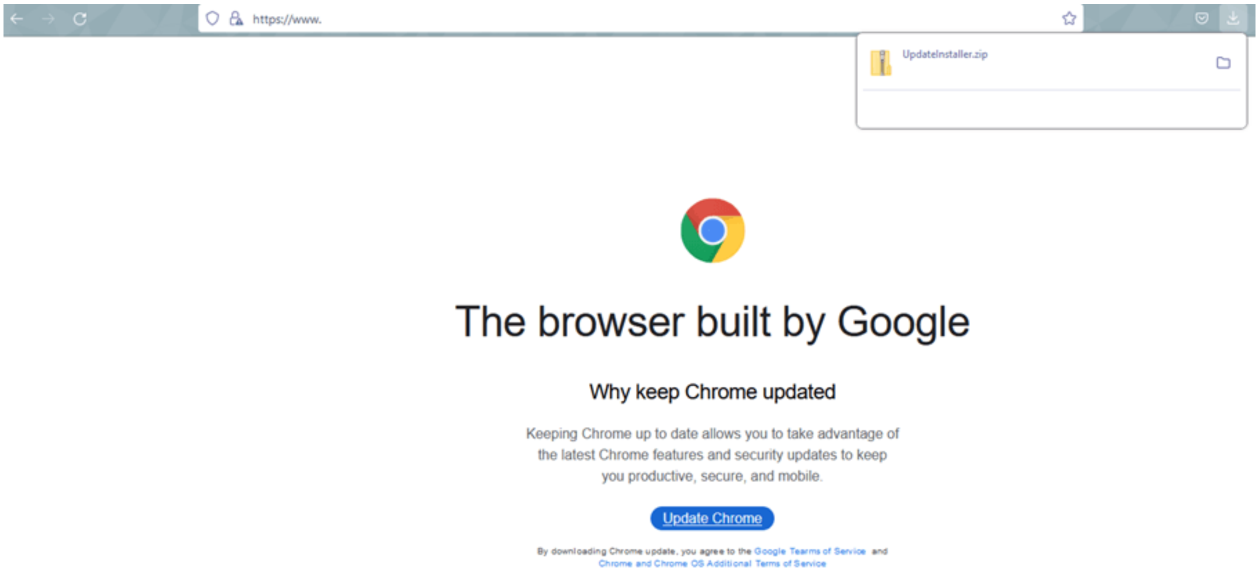
Introduction

The crimeware landscape is diverse. Cybercriminals try to capitalize on their victims in every possible way by distributing various types of malware designed for different platforms. In recent months, we have written private reports on a wide range of topics, such as new cross-platform ransomware, macOS stealers and malware distribution campaigns. In this article, we share excerpts from our reports on the FakeSG campaign, the Akira ransomware and the AMOS stealer.

To learn more about our crimeware reporting service, you can contact us at crimewareintel@kaspersky.com.

FakeSG

“FakeSG” is the name we gave to a new NetSupport RAT distribution campaign. The moniker was chosen as it mimics the notorious SocGholish distribution campaign. Legitimate websites are getting infected, displaying a notification that the user’s browser needs an update. For an example, look at the image below. Clicking the notification downloads a malicious file to the device. Over the course of time, the attackers have changed the download URL to stay undetected longer. However, for some obscure reason, the path has remained the same (/cdn/wds.min.php).



The browser built by Google

Why keep Chrome updated

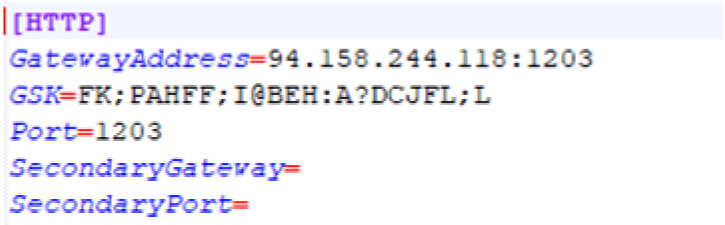
Keeping Chrome up to date allows you to take advantage of the latest Chrome features and security updates to keep you productive, secure, and mobile.

By downloading Chrome update, you agree to the Google Tearms of Service and Chrome and Chrome OS Additional Terms of Service

Landing page example

The download is a JS file that contains obfuscated code. When executed, it loads another script from a remote location and sets a cookie. Finally, it displays a prompt to update the browser and starts automatically downloading another script. This time, it is a batch script that downloads another batch script, a 7z file and the 7z executable.

The second batch script takes care of persistence by creating a scheduled task with the name “VCC_runner2”, extracts and copies the malware, and so on. Part of the 7z file is a malicious configuration file containing the address of the C2 (see the image below).



```
[HTTP]
GatewayAddress=94.158.244.118:1203
GSK=FK;PAHFF;I@BEH:A?DCJFL;L
Port=1203
SecondaryGateway=
SecondaryPort=
```

C2 address

Akira

Akira is a relatively new ransomware variant, first detected in this past April and written in C++, that can run in Windows and Linux environments. Despite the malware being relatively new, the attackers behind Akira are quite busy with over 60 confirmed infected organizations worldwide. In terms of targets, they choose larger organizations in various industries, such as retail, consumer goods, education, and others.

In many ways, Akira is no different from other ransomware families: shadow copies are deleted (using a combination of PowerShell and WMI); logical drives are encrypted, and certain file types and directories are skipped; there is a leak/communication site on TOR; and so on.

What sets it apart is certain similarities with Conti. For example, the list of folders excluded from the encryption process is exactly the same. This includes the “winnt” folder, which is only present in Windows 2000. Another similarity is the string obfuscation function used.

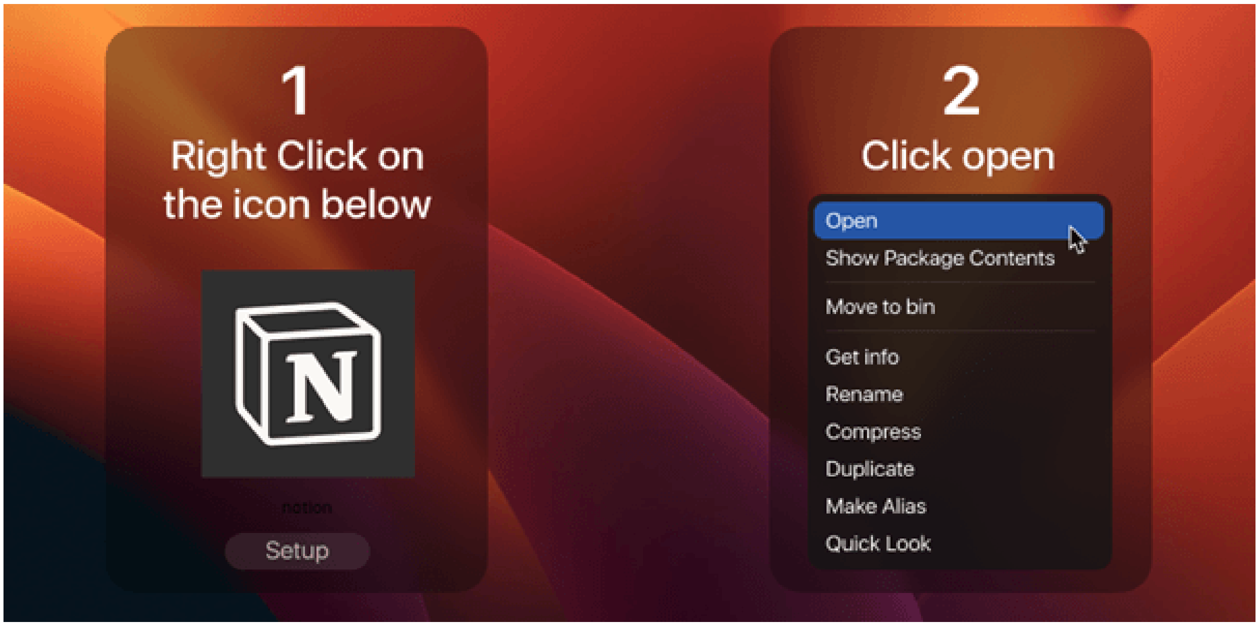
One thing that sets a group apart from another is the C2 panel. In the course of our investigations and joint effort with law enforcement agencies (LEAs) all around the world, we have come across many different types of C2 panels. Akira’s communication site, however, is something different. The group used the JQuery Terminal library to develop an old-skool minimalistic site. In order to protect it, they implemented certain security measures. For example, if you open the website while using a debugger in the browser, an exception will be raised, stopping the analysis.

AMOS

Stealers are growing in popularity. Certain famous stealers, such as Redline and Raccoon, have been around for years. Others emerged more recently, as we discussed in some of our previous blog posts. In the beginning of the year, we saw a number of new stealers appearing for macOS: XLoader, MacStealer, Atomic MacOS aka AMOS and others.

AMOS was first discovered in April 2023. At that time it was leased to cybercriminals via Telegram for 1000$ per month. The initial version, written in Go, had typical stealer features, such as stealing passwords, files, browser data and so on. It also created fake password prompts in an attempt to obtain the system password.

The new version changed a few things, most notably, the programming language. AMOS is now written in C instead of Go. We also were able to determine the infection vector: malvertising. Similarly to the Redline and Rhadamantys campaigns, popular software sites get cloned, and users are lured into downloading the malware. The downloaded file is a DMG image that contains instructions on how to install the malware as can be seen in the image below.



1 Right Click on the icon below

2 Click open

Malware installation instructions

The first thing the malware does is retrieve the user name and check if the password is blank or no password is required. If the password is required and the user is not logged in, the malware creates a popup using osascript, asking to enter the password. Once all is set, the following data will be collected:

- Notes database
- Documents from the desktop and Documents
- Browser-related data (cookies, login data, and so on) from browsers like Chrome and Edge
- Cryptocurrency wallets (Binance, Exodus and others)
- Instant messaging data (Telegram, Discord and so on)

The data is zipped with the “miniz” library and sent to the C2 over HTTP. Part of the request is the UUID identifying the malware buyer or campaign.

In terms of victimology, we have detected infections all around the world, with Russia and Brazil targeted the most heavily.

If you would like to stay up to date on the latest TTPs being used by criminals, or if you have questions about our private reports, you can contact us at crimewareintel@kaspersky.com.

Indicators of compromise

NetSupportManagerRAT
C60AC6A6E6E582AB0ECB1FDBD607705B

Akira
00141f86063092192baf046fd998a2d1
0885b3153e61caa56117770247be0444
2cda932f5a9dafb0a328d0f9788bd89c

AMOS
3d13fae5e5febfa2833ce89ea1446607e8282a2699aafd3c8416ed085266e06f
9bf7692f8da52c3707447deb345b5645050de16acf917ae3ba325ea4e5913b37

- Apple MacOS
- crimeware
- Cross-platform malware
- Cybercrime
- Malware
- Malware Descriptions
- Malware Technologies
- Malware-as-a-Service
- Ransomware
- RAT Trojan
- Trojan
- Trojan-stealer

Authors

GReAT

FakeSG campaign, Akira ransomware and AMOS macOS stealer

Your email address will not be published. Required fields are marked *