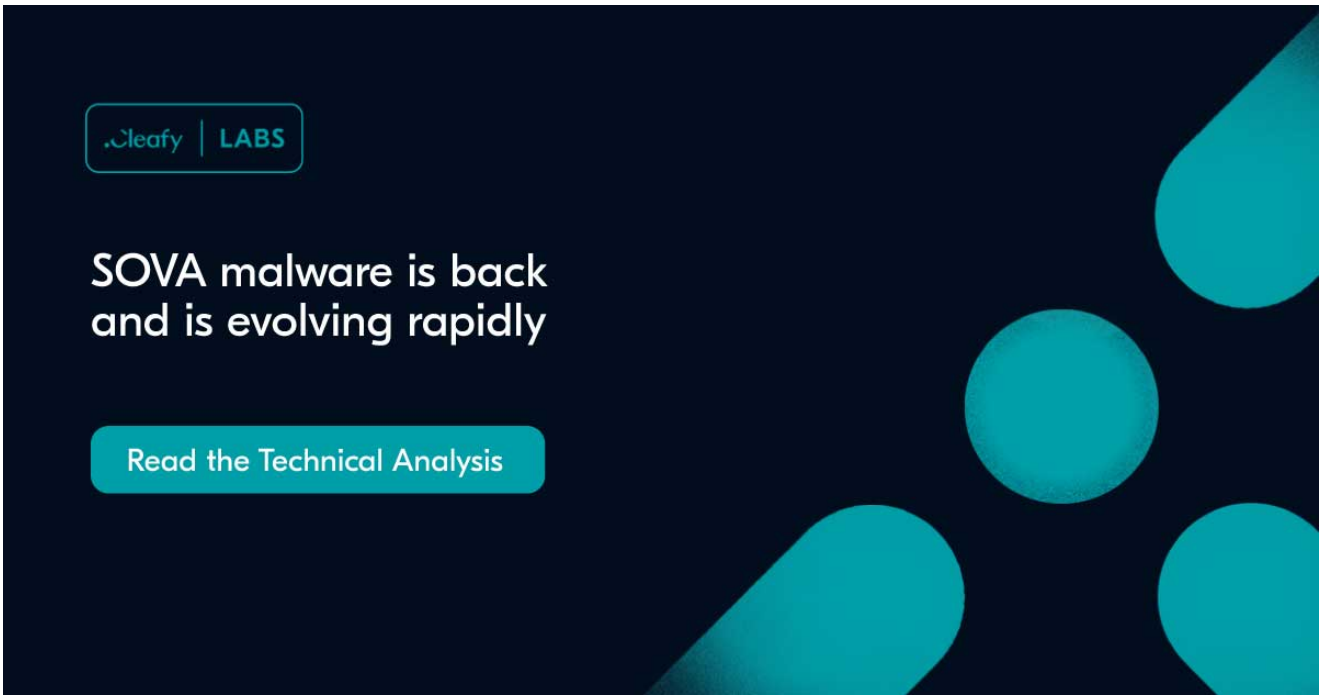
SOVA malware is back and is evolving rapidly

cleafy.com/cleafy-labs/sova-malware-is-back-and-is-evolving-rapidly

Francesco Iubatti, Federico Valentini



Download your PDF guide to TeaBot

Get your free copy to your inbox now

Download PDF Version

Introduction

In September 2021, SOVA, a new Android Banking Trojan, was announced in a known underground forum. Even though at that time the author claimed the malware was still under development, it actually already had multiple capabilities and was basically almost in the go-to market phase.

Furthermore, the authors of SOVA showed a roadmap with the future update of the malware as shown in Figure 1.

Coming soon:
1. automatic 3stage injections
2. Automatic cookie injections
3. Finish normal clipper
4. DDOS
5. GIF accessibility
6. Improving Panel Health
7. Ransomware (inject for card number)
8. Internet Packet Grabber (packet capture, "MITM" attack)
9. Normal PUSH notifications
10. Many injects
11. VNC
12. 2FA interception

Our bot is still under testing/development, but we have decided that we are ready to enter the market.

Figure 1 – Roadmap of SOVA (September 2021)

Until March 2022, multiple versions of SOVA were found and some of these features were already implemented, such as: 2FA interception, cookie stealing and injections for new targets and countries (e.g. multiple Philippine banks).

In July 2022, we discovered a new version of SOVA (v4) which presents new capabilities and seems to be targeting more than 200 mobile applications, including banking apps and crypto exchanges/wallets.

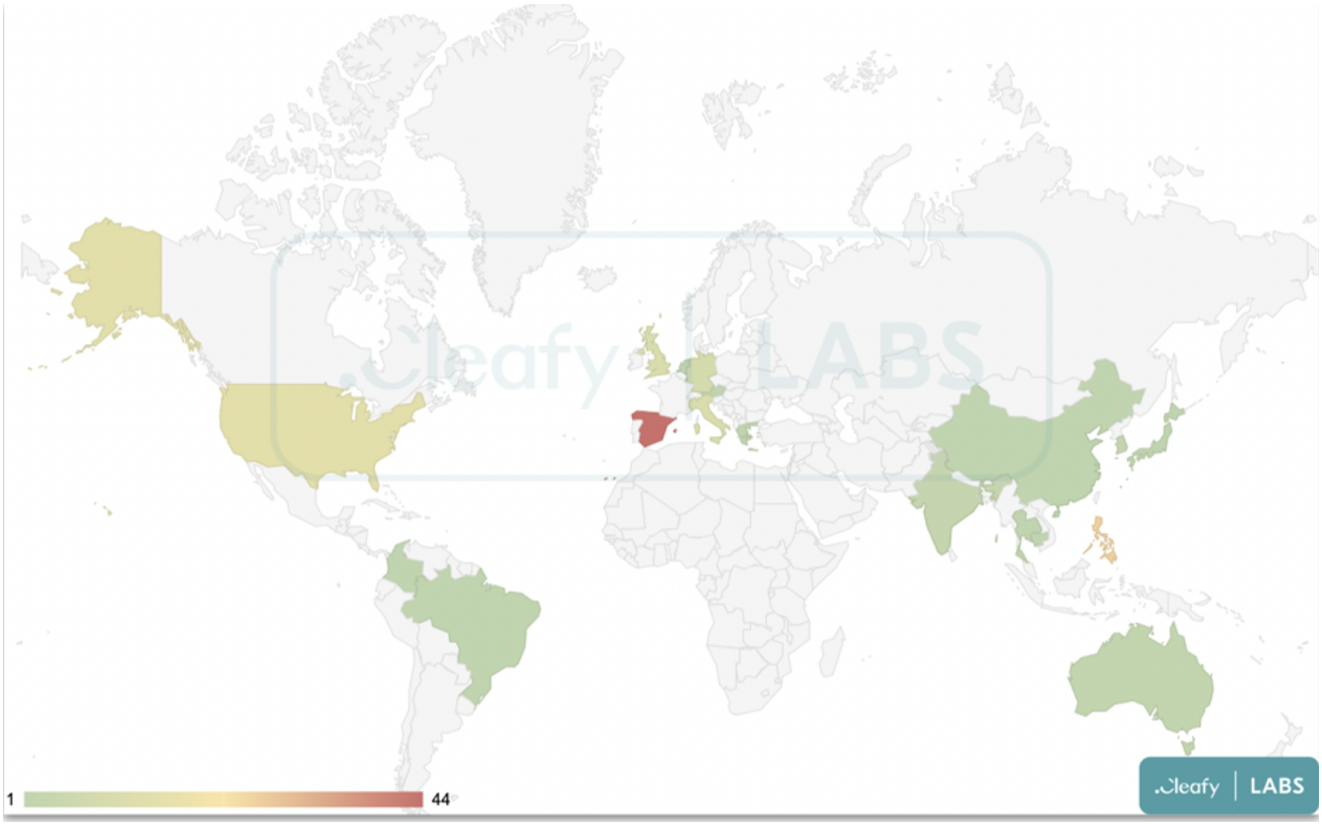


Figure 2 – Main countries targeted by SOVA v4

Updates - SOVA v4

Starting from May 2022, Threat Actors (TAs) behind SOVA have started to deliver a new version of their malware, hiding within fake Android applications that show up with the logo of a few famous ones, like Chrome, Amazon, NFT platform or others.

Figure 3 – Main icons used by SOVA v4

Differently from the previous versions, this time several new codes were added. The most interesting part is related to the VNC capability. As shown in Figure 1, this feature has been in the SOVA roadmap since September 2021 and that is one strong evidence that TAs are constantly updating the malware with new features and capabilities.

Starting from SOVA v4, TAs can obtain screenshots of the infected devices, to retrieve more information from the victims. Furthermore, the malware is also able to record and obtain any sensitive information, as shown in Figure 5. These features, combined with Accessibility services, enable TAs to perform gestures and, consequently, fraudulent activities from the infected device, as we have already seen in other Android Banking Trojans (e.g. Oscorp or BRATA).

With SOVA v4, TAs are able to manage multiple commands, such as: screen click, swipe, copy/paste and the capability to show an overlay screen to hide the screen to the victim. However, it was observed that multiple logs information are still sent back to the C2. This behavior is a strong indicator that SOVA is still going through a development process, while TAs are rolling out new features and capabilities.

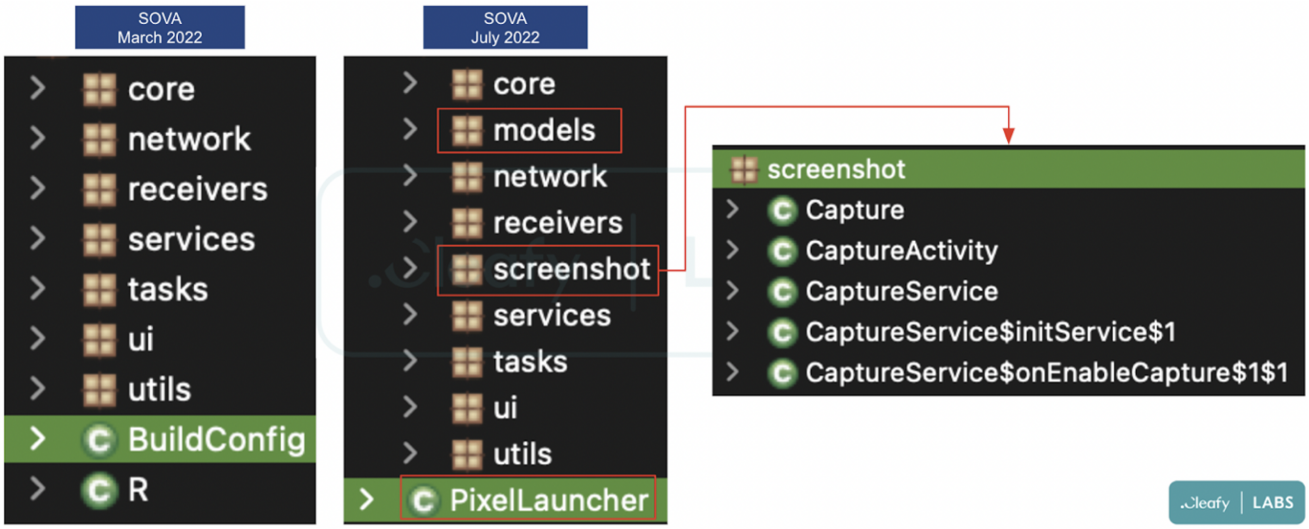


Figure 4 – Code comparison between SOVA v3 and v4

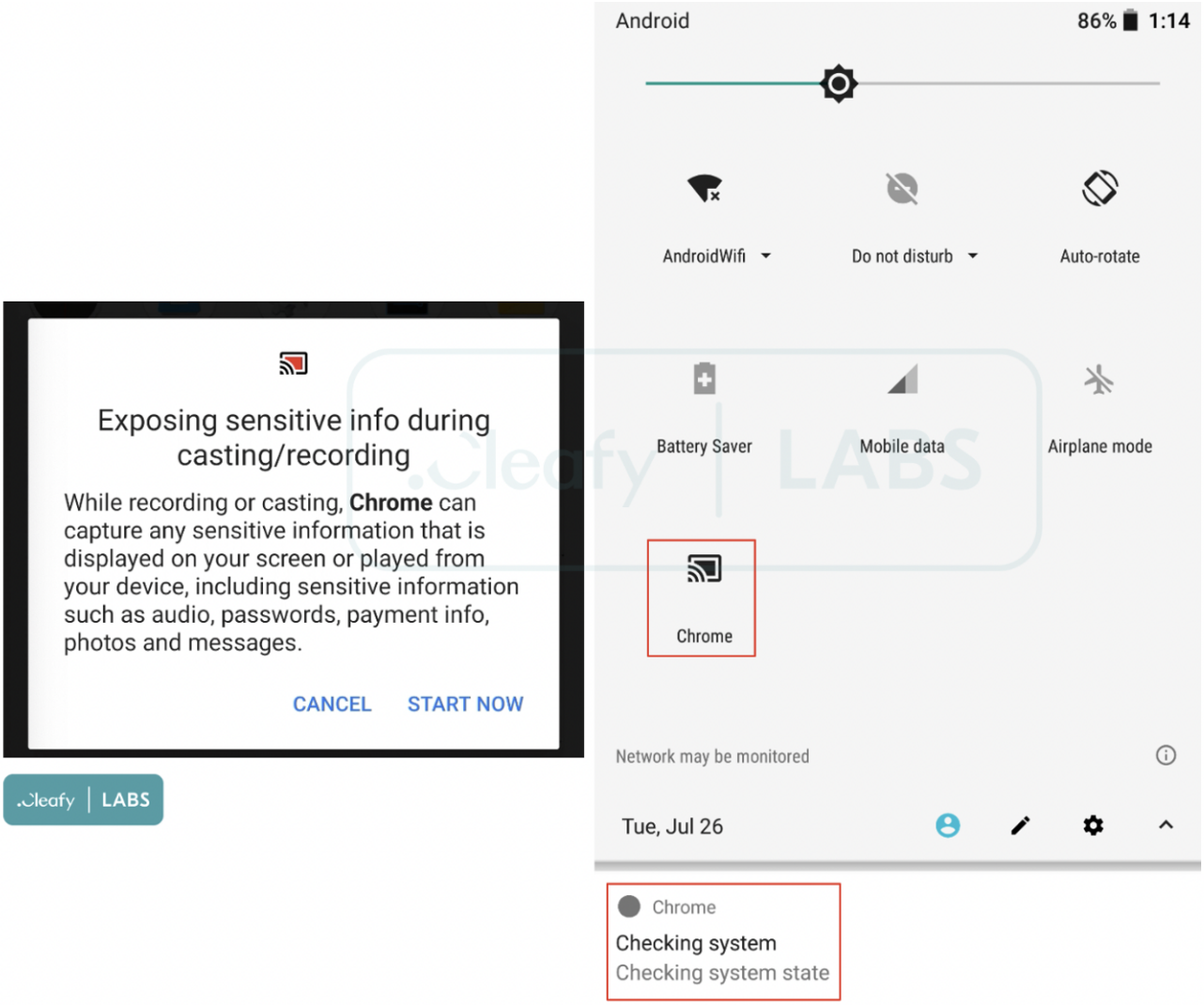


Figure 5 – Casting/Recording feature of SOVA v4

Moreover, in SOVA v4, the cookie stealer mechanism was refactored and improved. In particular, TAs specified a comprehensive list of Google services that they are interested to steal (e.g. Gmail, GPay, and Google Password Manager), plus a list of other applications.

For each of the stolen cookies, SOVA will also collect additional information such as “is httpOnly”, its expiration date, etc.

Figure 6 – Refactoring and improvement of the cookie stealer mechanism in SOVA v4

Another interesting update about SOVA v4 is the refactoring of its “protections” module, which aims to protect itself from different victim’s actions. For example, if the user tries to uninstall the malware from the settings or pressing the icon, SOVA is able to intercept these actions and prevent them (through the abuse of the Accessibilities) by returning to the home screen and showing a toast (small popup) displaying *“This app is secured”*.

Figure 7 – “Protections” code comparison between SOVA v3 and v4

A peculiarity of SOVA v4 is the “core” relocation of the malware. Like the main Android banking trojan, SOVA uses the .apk just to unpack a .dex file which contains the real malicious functionalities of the malware. In the previous version, SOVA stored the .dex file inside the directory of the app, while in the current version it uses a device's shared storage directory (“Android/obb/”) to store it.

Lastly, in SOVA v4, an entire new module was dedicated to **Binance** exchange and the **Trust Wallet** (official crypto wallet of Binance). For both applications, TAs aim to obtain different information, like the balance of the account, different actions performed by the victim inside the app and, finally, even the seed phrase (a collection of words) used to access the crypto wallet.

C2 communications and panel

The communications between SOVA v4 and the C2 didn’t change compared to the previous version (v3), except for the new command (vncinfo) used for its new VNC feature. Meanwhile, also the C2 panel of SOVA was updated compared to the first version published by the author in September 2021, with some new features and a complete UI restyle (as shown in Figure 8).

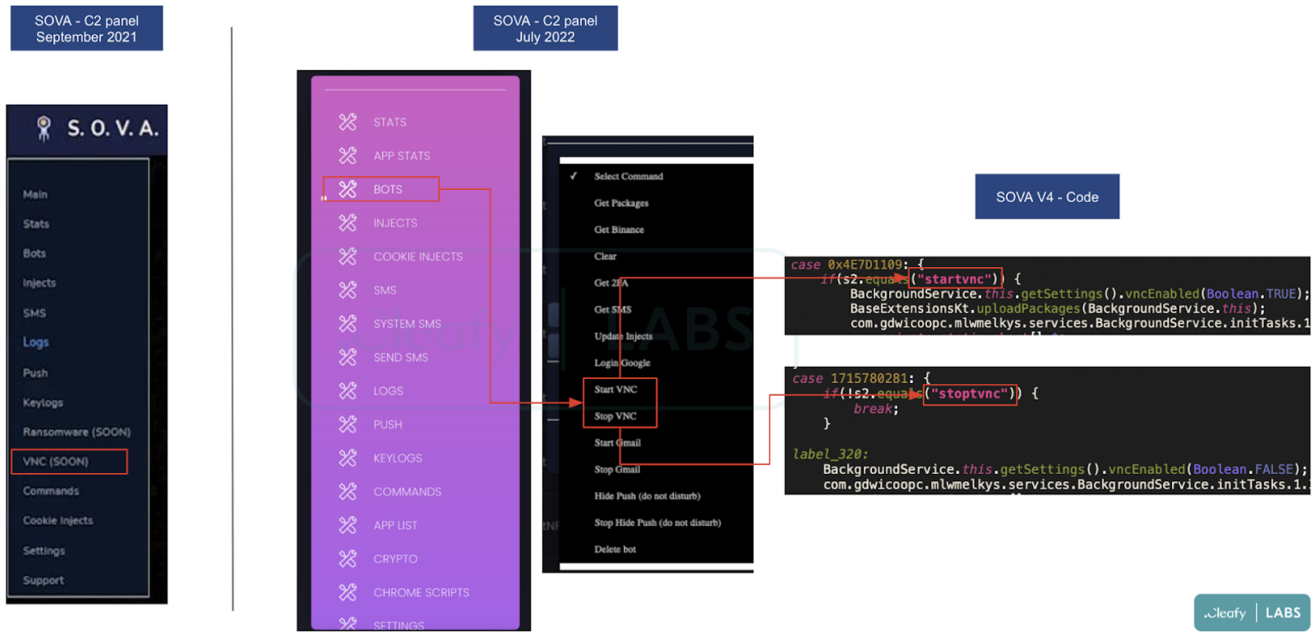


Figure 8 – Comparison between SOVA C2 panels

Sova - March 2022

```
public static {
    Config.$ = new short[]{2130, 0x855, 0x849, 0x84E, 0x1C8
    Config.INSTANCE = new Config();
    d0.c(BuildConfig.HOST, "HOST");
    Config.host = "https://xireycicin.xyz";
    d0.c(BuildConfig.KEY, "KEY");
    Config.key = "lelelo";
    Config.firstList = a.k(new String[]{"com.android.vendin
    Config.secondList = a.k(new String[]{"com.android.chrom
}
```

Sova - July 2022

```
public static {
    Config.$ = new short[]{0x2F49, 0x2F45, 0x2F47, 0x2F04, 0x2F4B, 12100
    Config.host = "https://socrersutagans.site";
    Config.key = "foh";
    Config.notifyMessage = "Checking system state";
    Config.notifyTitle = "Checking system";
    Config.INSTANCE = new Config();
    Config.mode = AppModeType.App;
    Config.gLogin = true;
    Config.firstList = a.k(new String[]{"com.android.vending", "com.goog
    Config.secondList = a.k(new String[]{"com.android.chrome", "com.twit
    Config.vncHost = "http://81.19.139.34:1080";
    Config.launchProtected = true;
}
```

Figure 9 – Comparison between SOVA configuration files

New Targets

The first version of SOVA had almost 90 targeted applications (including banks, crypto wallet/exchange, and generic shopping apps), initially listed and stored in the packageList.txt file within the assets/ folder. In the latest samples, this file has been removed and the targeted applications are managed through the communications between the malware and the C2.

The number of targeted applications has grown faster, compared to the initial phases of SOVA: during March 2022 multiple Philippine banks have been added and then during May 2022, another list of banking applications has been added too, as shown in the following Figure 10.

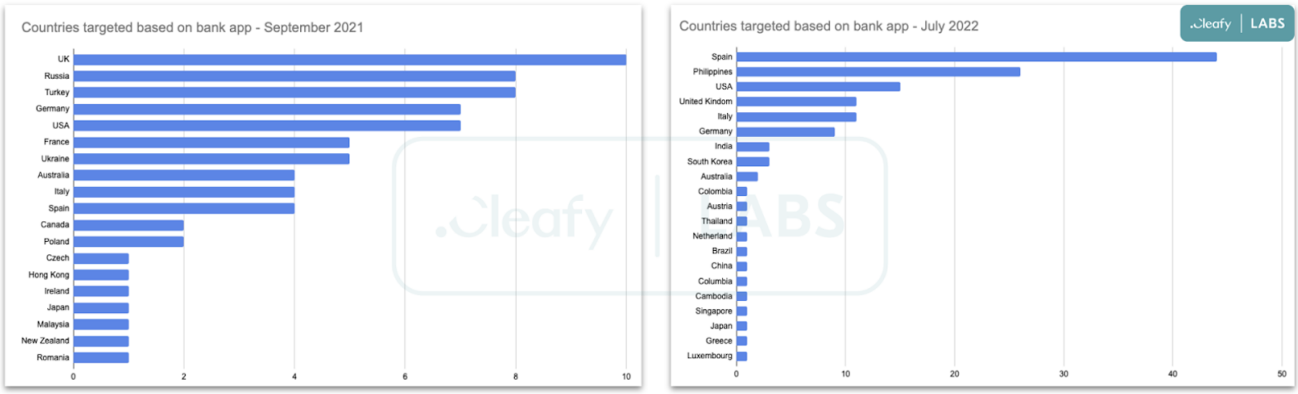


Figure 10 – Comparison between SOVA targets, from September 2021 to July 2022

To obtain the list of targeted applications, SOVA sends the list of all applications installed on the device to the C2, right after it has been installed. At this point, the C2 sends back to the malware the list of addresses for each targeted application and stores this information inside an XML file.

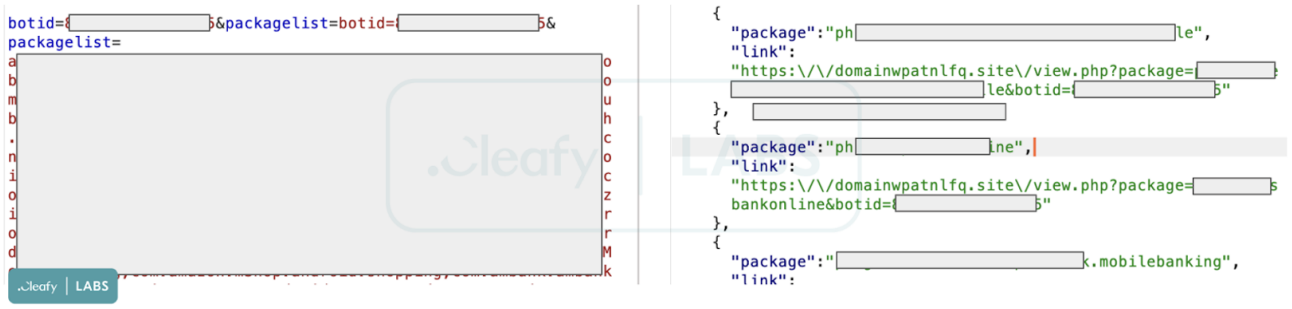


Figure 11 – Example of communication between SOVA v4 and the C2 server

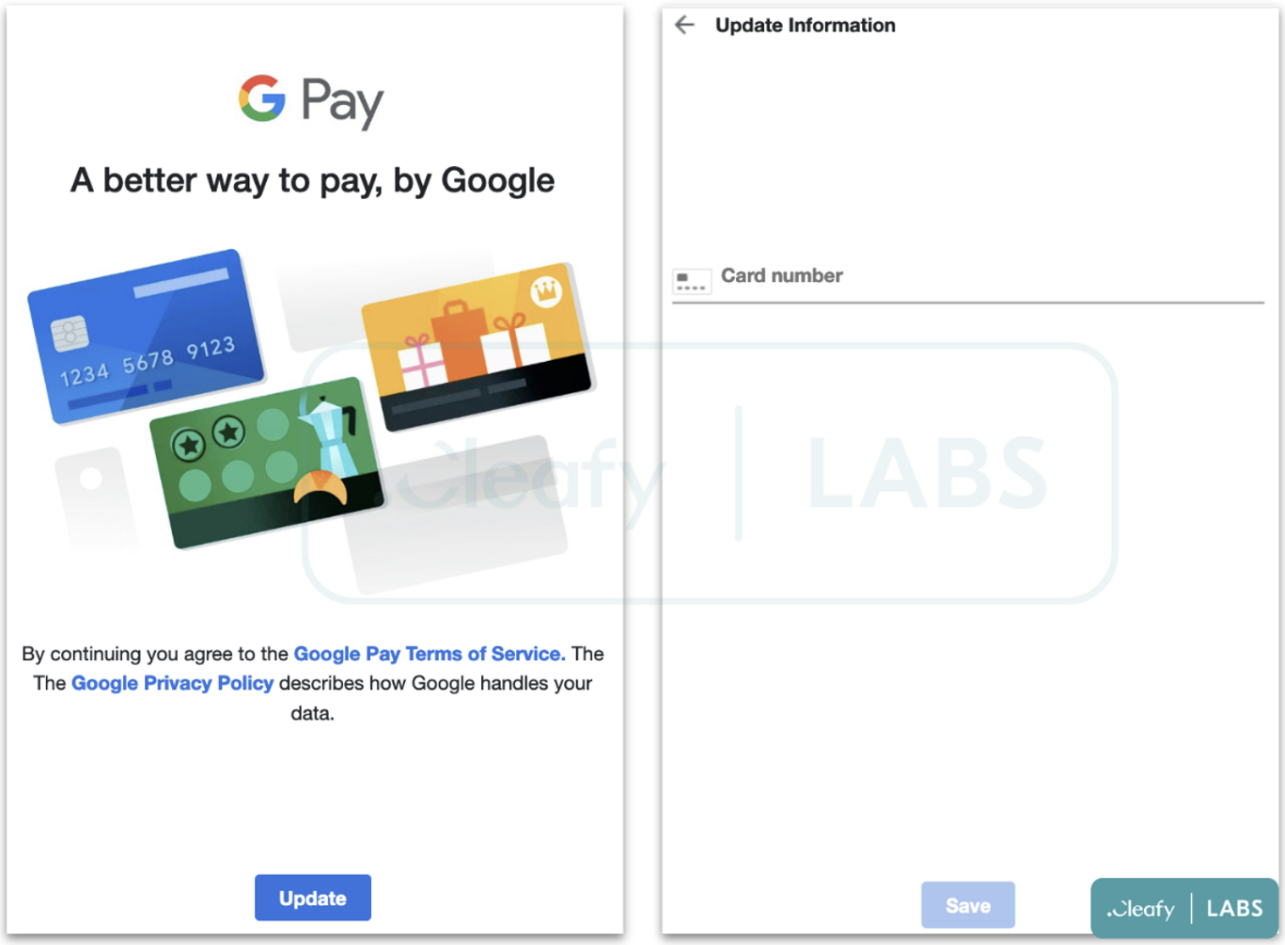


Figure 12 – Example of fake page used to steal credentials and credit card information

Another interesting fact is that, in some of the analyzed samples of SOVA v4, the list of CIS region used in the previous versions (used to exclude these countries from attacks) was removed and, at the time of writing, all the initial Russian and Ukraine targeted apps were removed.

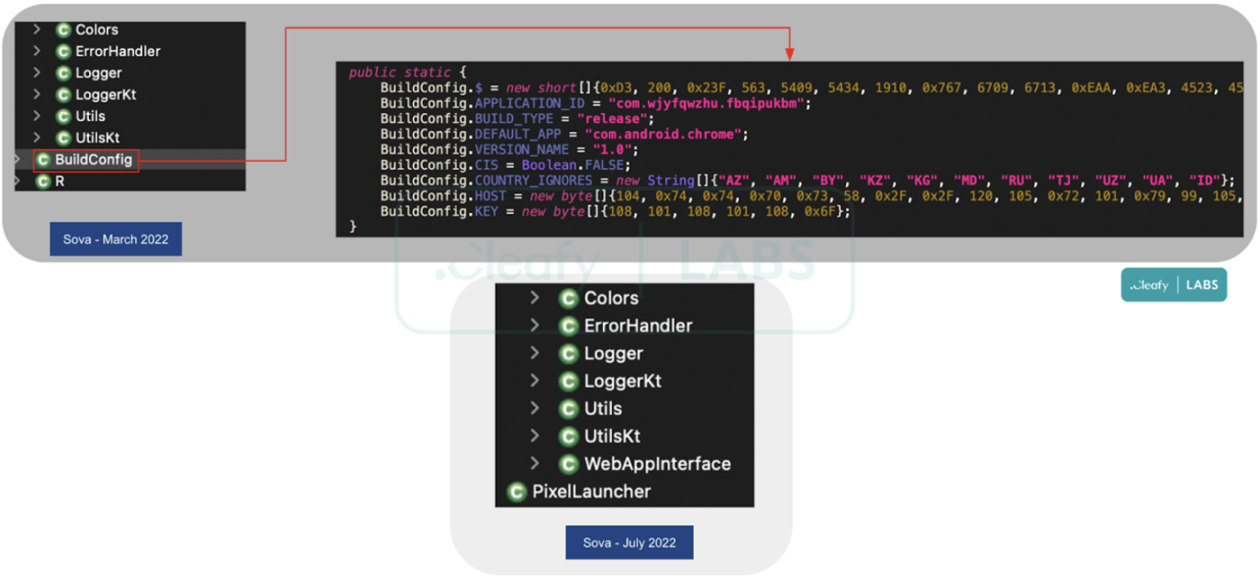


Figure 13 – List of CIS region remove in one of the sample of SOVA v4

Further updates - SOVA v5

During the reviewing of the document on SOVA v4, we spotted on our threat intelligence platform (Cleafy ASK) multiple samples that seem to belong to a further variant of SOVA (v5); we want to provide you with an overview of this variant too.

Analyzing the code of the malware, it is possible to observe a big refactoring of the code, the addition of new features and some small changes in the communications between the malware and the C2 server. Furthermore, the samples of SOVA v5 that we analyzed don't present the VNC module that we observed in SOVA v4: our hypothesis is that it was simply not integrated in the v5version yet. In fact, the malware seems to be still under development, due to the presence of multiple logs used for debugging.

Figure 14 – List of commands of SOVA v5

Although there are several changes, the most interesting features added in SOVA v5 is the ransomware module, that was announced in the roadmap of September 2021.

However, even though this feature has been already implemented in the current version (v5), at the time of writing it seems to be still under development.

The aim of TAs is to encrypt the files inside the infected devices through an AES algorithm and renaming them with the extension ".enc".

The ransomware feature is quite interesting as it's still not a common one in the Android banking trojans landscape. It strongly leverages on the opportunity arises in recent years, as mobile devices became for most people the central storage for personal and business data.

Figure 15 – Ransomware module of SOVA v5

Conclusions

With the discovery of SOVA v4 and SOVA v5, we uncovered new evidence about how TAs are constantly improving their malware and the C2 panel, honouring the published roadmap.

Although the malware is still under development, it's ready to carry on fraudulent activities at scale.

Appendix 1: IOCs

IoC	Description
0533968891354ac78b45c486600a7890	SOVA v4
ca559118f4605b0316a13b8cfa321f65	SOVA v4 without CIS regions
socrersutagans.]site	C2 of SOVA v4
omainwpatnlfq.]site	Server used to display fake website of targeted app
74b8956dc35fd8a5eb2f7a5d313e60ca	SOVA v5
satandemantenimiento.com	C2 of SOVA v5
http://wecrvtbyutrcewwretyntrverfd.xyz	C2 of SOVA v5