

Mobile banking fraud: BRATA strikes again

By Federica Abbinante, Francesco Iubatti

Archived: 2026-04-05 14:24:38 UTC

Executive Summary

In the past year, we observed in the Cleafy platform a spike of Android RAT infections caused by the increase of Android Banking Trojan used to perform fraudulent activities, usually combined with smishing and social engineering attack patterns. Simultaneously, we noticed a decrease in SIM swap attacks, possibly related to the fact that they are less scalable than the widely used malware as a service (MaaS) pattern.

What makes Android RAT so interesting for attackers is its capability to operate directly on the victim devices instead of using a new device. By doing so, Threat Actors (TAs) can drastically reduce the possibility of being flagged "as suspicious", since the device's fingerprinting is already known to the bank.

In this report, we analyze the attack chain and the modus operandi used by Threat Actors, from the sending of the malicious SMS to the fraudulent transaction carried out through an app installed in the infected device.

Moreover, we highlight the main indicators to explain the attack chain used by these TAs:

- The malware campaign targets mainly one of the biggest Italian retail banks as well as other minor banks. However, we don't exclude that other local TAs might be using the same attack vector (BRATA) to carry over other malicious activities in other countries.
- Smishing and phishing attacks are used to distribute malicious apps and credentials harvesting.
- A new version of the BRATA malware is used to infect the device of the victims.
- A combination of both social engineering techniques and the complete control of the infected device is used by TAs to perform fraudulent transactions.

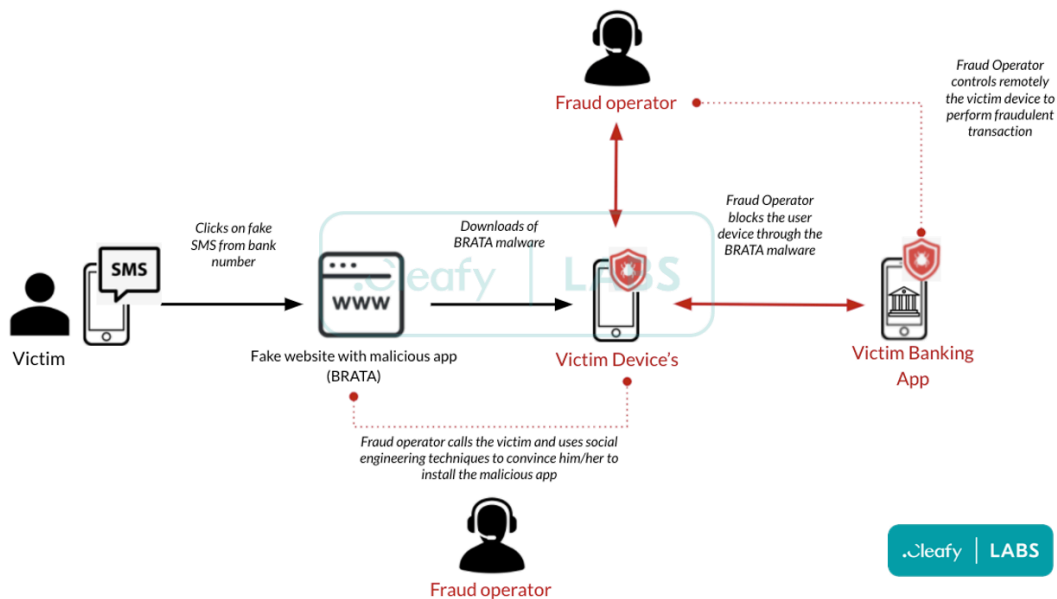


Figure 1 - BRATA distribution and modus operandi

Introduction

At the end of June 2021, the Cleafy Threat Intelligence and Incident Response team intercepted for the first time a new aggressive smishing campaign that was delivering multiple fake applications called “**Sicurezza Dispositivo**” (or “**AntiSPAM**”). The campaign targeted the customers of one of the biggest Italian retail banks.



2021-09-15 17:58:22	2021-09-15 17:58:28	com.rockstar.gta3	Sicurezza Dispositivo	2
2021-09-08 16:41:41	2021-09-08 16:59:02	com.rockstar.gta3	Sicurezza Dispositivo	14
2021-09-08 12:19:54	2021-09-15 13:15:38	com.rockstar.gta3	Sicurezza Dispositivo	86
2021-09-06 16:36:43	2021-09-16 10:14:33	b4a.example	Sicurezza Dispositivo	14
2021-09-03 16:55:55	2021-09-03 17:00:20	b4a.example	Sicurezza Dispositivo	8
2021-09-03 13:15:35	2021-09-03 17:46:45	b4a.example	Sicurezza Dispositivo	56
2021-09-02 20:25:12	2021-09-02 22:41:30	b4a.example	Sicurezza Dispositivo	6
2021-09-01 13:31:59	2021-09-02 15:56:45	b4a.example	Sicurezza Dispositivo	118
2021-08-31 15:15:21	2021-08-31 16:28:28	b4a.example	Sicurezza Dispositivo	26
2021-08-12 14:26:58	2021-08-12 14:28:47	b4a.example	Sicurezza Dispositivo	6
2021-08-10 16:32:13	2021-08-18 17:57:58	b4a.example	Sicurezza Dispositivo	302
2021-08-04 15:18:30	2021-08-04 16:42:35	b4a.example	Sicurezza Dispositivo	20
2021-07-28 16:40:46	2021-08-06 16:27:50	b4a.example	Sicurezza Dispositivo	17
2021-07-26 16:35:25	2021-08-06 14:29:08	b4a.example	Sicurezza Dispositivo	186
2021-07-21 14:06:57	2021-09-10 15:32:52	b4a.example	Sicurezza Dispositivo	532
2021-07-21 13:24:19	2021-07-21 13:41:12	b4a.example	Sicurezza Dispositivo	12
2021-07-20 15:20:56	2021-07-20 16:58:03	b4a.example	Sicurezza Dispositivo	182
2021-07-06 17:32:49	2021-07-15 17:54:01	b4a.example	Sicurezza Dispositivo	6
2021-07-05 20:52:09	2021-07-05 20:52:14	com.example	Sicurezza Dispositivo	2
2021-06-21 16:30:26	2021-09-15 15:36:42	opedrt.eelrltoq.eoxmae	Sicurezza Dispositivo	636

Figure 2 - Some BRATA samples and related occurrences

After the first wave, lasted from June to mid-September, the attack stopped for about a month. In mid-October, our TIR team discovered that new samples called “**Sicurezza Avanzata**” were again in action and were targeting mainly the customers of three Italian banks. This time the malware was almost undetectable by antivirus solutions (as shown in Figure 3).



Figure 3 - Difference between two BRATA samples detected by antivirus solutions

How the BRATA malware works

In June 2021, for the first time we detected on Cleafy’s dashboards a new variant of BRATA malware. After a couple of weeks, a customer reported to us some incidents related to the same campaign.

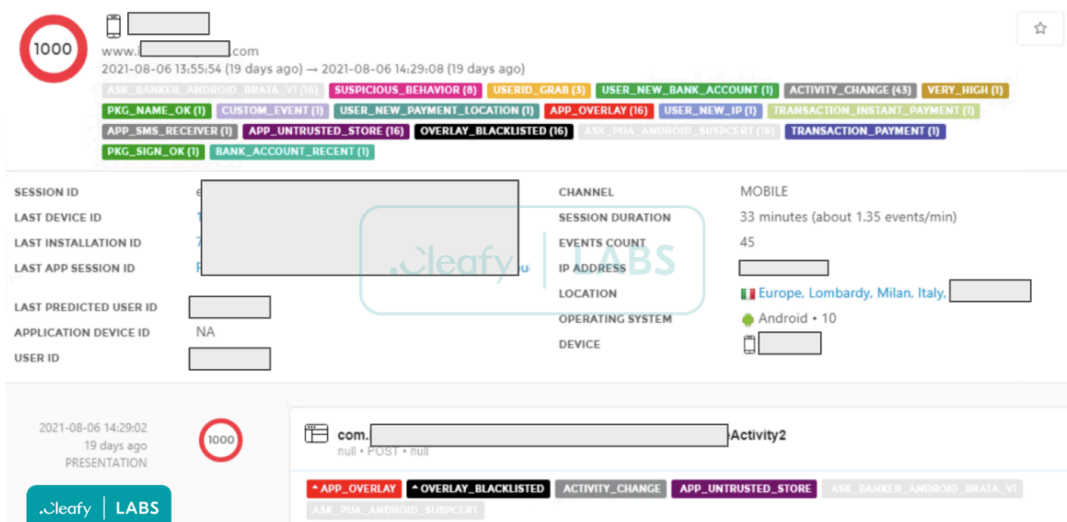


Figure 4 - Example of BRATA malware intercepted and blacklisted in Cleafy console

Thanks to an in-depth technical analysis of the Indicators of Compromise intercepted, we were able to reconstruct the detailed chain of events and the methodologies used by these Threat Actors to conduct bank frauds.

The attack chain usually starts with a fake SMS containing a link to a website. The SMS seems to come from the bank (the so-called spoofing scam), and it tries to convince the victim to download an anti-spam app, with the promise to be contacted soon by a bank operator.

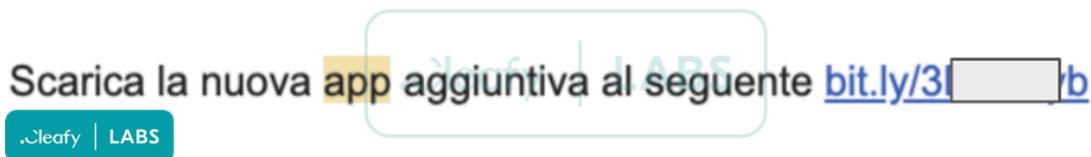


Figure 5 - Example of one of the SMS received from the victim

In some cases, the link redirects the victim to a phishing page that looks like the bank's, and it is used to steal credentials and other relevant information (e.g. fiscal code and security questions).

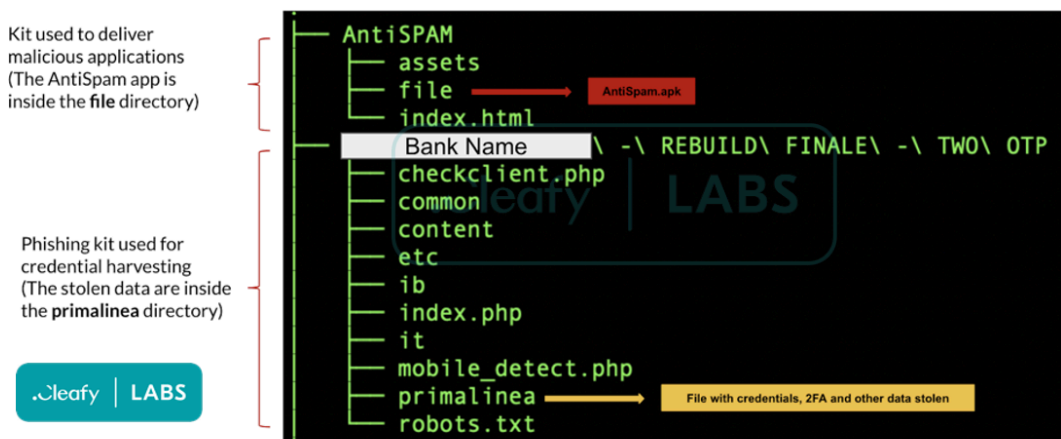


Figure 6 - Phishing kit used by TAs to deliver BRATA and for credential harvesting

```
-----
|              NUOVO LOGIN              |
|-----|
| Codice Titolare: [redacted]51         |
| PIN: [redacted]                       |
| Nome: [redacted]                      |
| Cognome: [redacted]                   |
| Codice Fiscale: GHZD[redacted]        |
| Cellulare: 347[redacted]              |
| IP: 37.[redacted]                     |
| User-Agent: Mozilla/5.0 (Linux; Android 7.0; SAMSUNG SM-G920F) AppleWebKit/537.36 |
|-----|
|+++++|
| DOMANDE DI SICUREZZA PER [redacted]51 |
|-----|
| Domanda 1: Qual è il nome del tuo migliore amico? |
| Risposta 1: [redacted]                  |
| Domanda 2: Qual era il tuo cantante o gruppo preferito quando eri piccolo? |
| Risposta 2: [redacted]                  |
| Domanda 3: Qual è il nome della tua squadra preferita? |
| Risposta 3: [redacted]                  |
| IP: 37.16[redacted]                    |
| User-Agent: Mozilla/5.0 (Linux; Android 7.0; SAMSUNG SM-G920F) AppleWebKit/537.36 |
|-----|
| [!!!] [1] PRIMO CODICE OTP PER [redacted]51 -----> 81865 |
| [!!!] [2] SECONDO CODICE OTP PER [redacted]51 -----> 317091 |
|-----|
```



Figure 7 - Example of information stolen by BRATA group

After the victim visits the website (only visible via mobile[1]) and downloads the malicious app, a fraud operator calls the victim and uses social engineering techniques to persuade the user to install the malicious app.

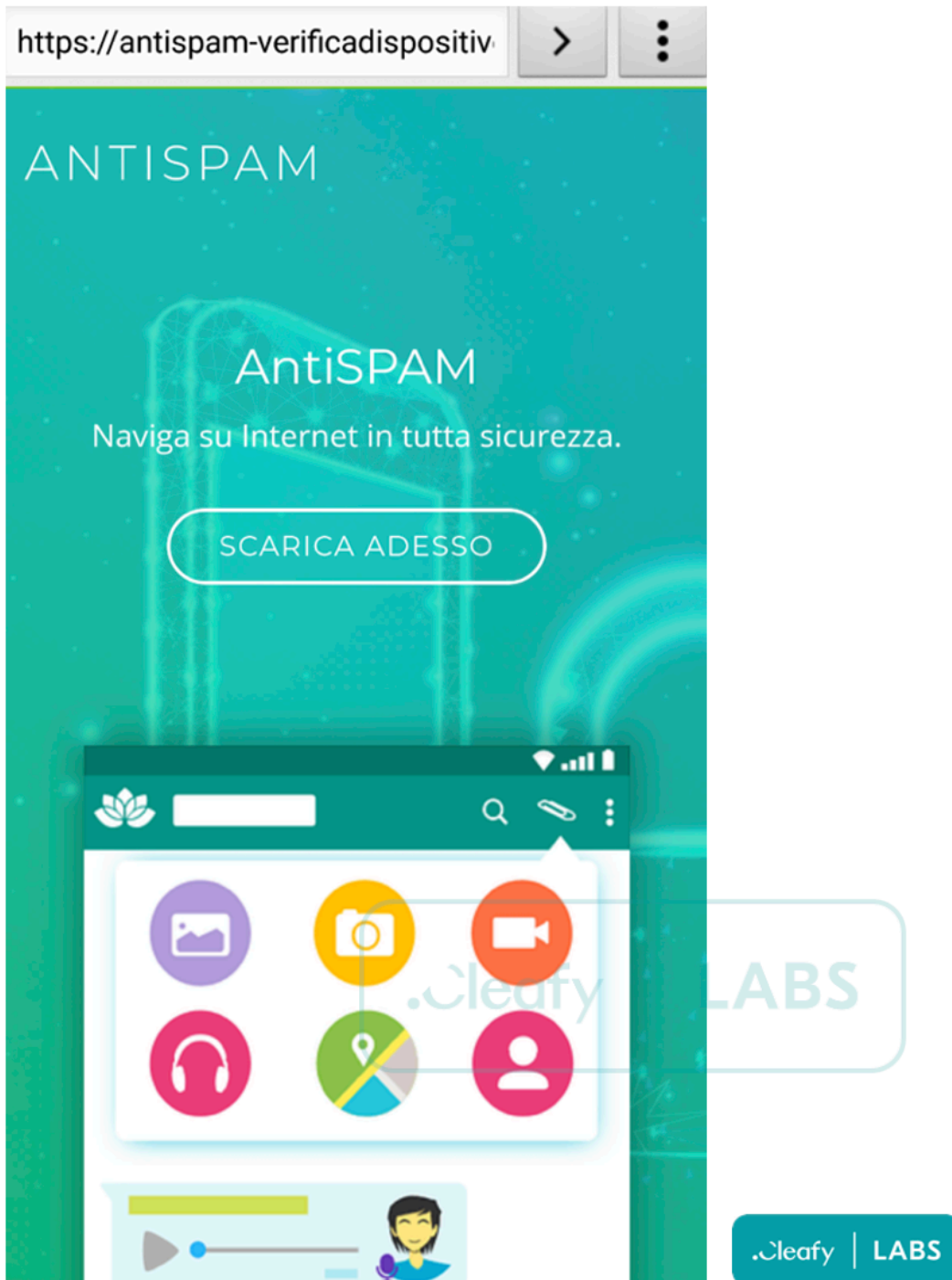


Figure 8 - Example of website used to spread BRATA malware in Italy

During the installation phases of the malware (Figure 9), multiple permissions are required to allow the attackers to perform fraudulent activities.

Once the malicious app is installed, the fraud operators can take control of the victim infected devices thanks to the abuse of the Accessibility services, the SMS permission, and the recording/casting module of the malware.

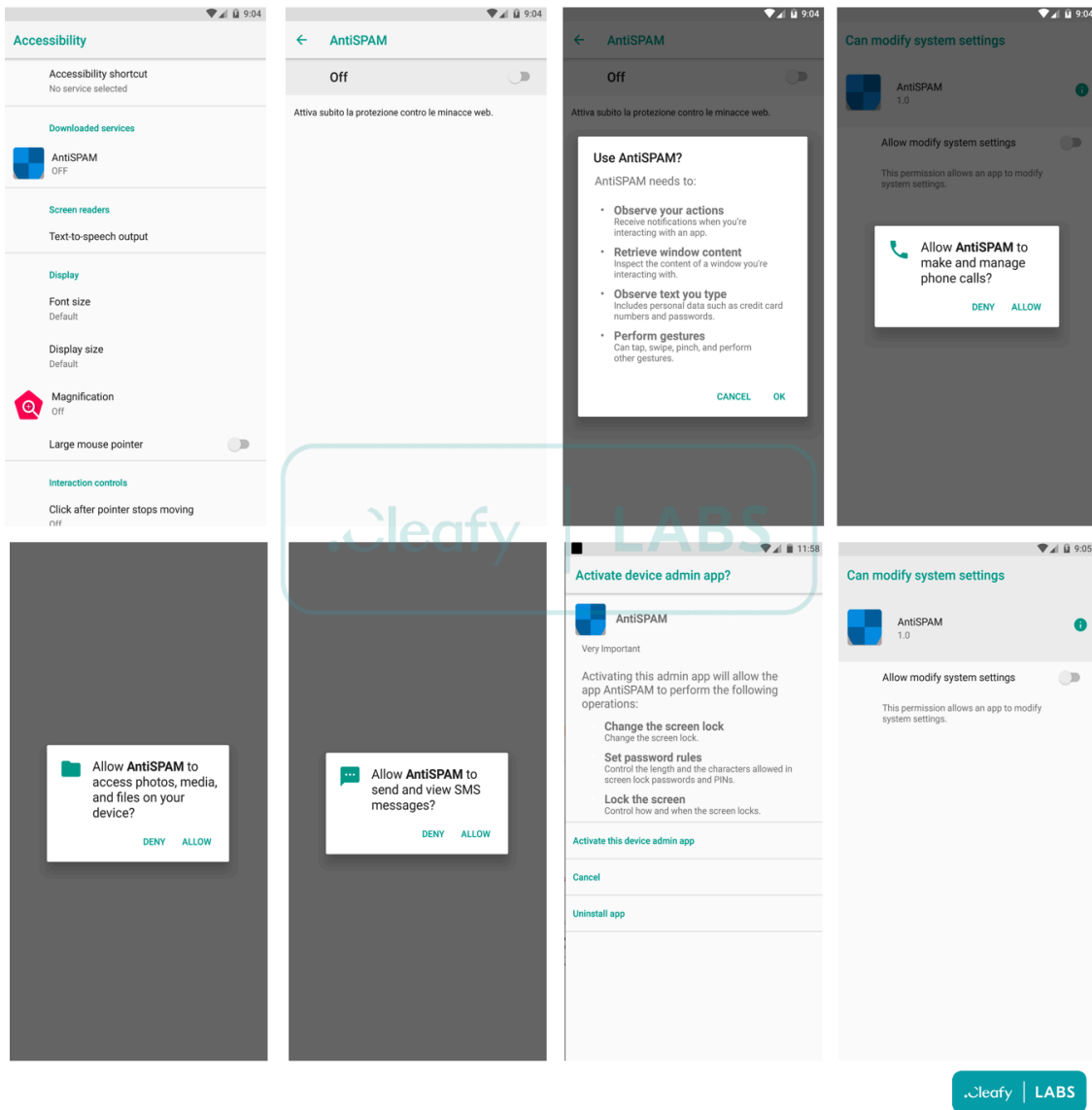


Figure 9 - Installation phase of BRATA malware on Android device

Through the malware installed on the victim device, Threat Actors can receive on their server the 2FA code sent by the bank and perform fraudulent transactions. Therefore, as we observed also in other scenarios, with the abuse of Accessibility Service and the screen recording, TAs can perform actions on the infected device with the help of social engineering used to persuade the victim.



Figure 10 - Example of fraud transactions performed by TAs inside the infected device

As shown in Figure 11, we also intercepted multiple attempts of pin/otp validations stolen by TAs through the malicious app (or phishing website). This specific pattern was observed also in other past campaigns of mobile and workstation malware.



Figure 11 - Attempt to use stolen credentials intercepted in Cleafy Console

The mule accounts used by the BRATA malware campaign mainly come from Italy, as well as from Lithuania and the Netherlands, as shown in Figure 12. From this information, we assume that the TAs behind these campaigns could come from European countries unlike the previous BRATA malware campaign observed in Brazil in 2019.

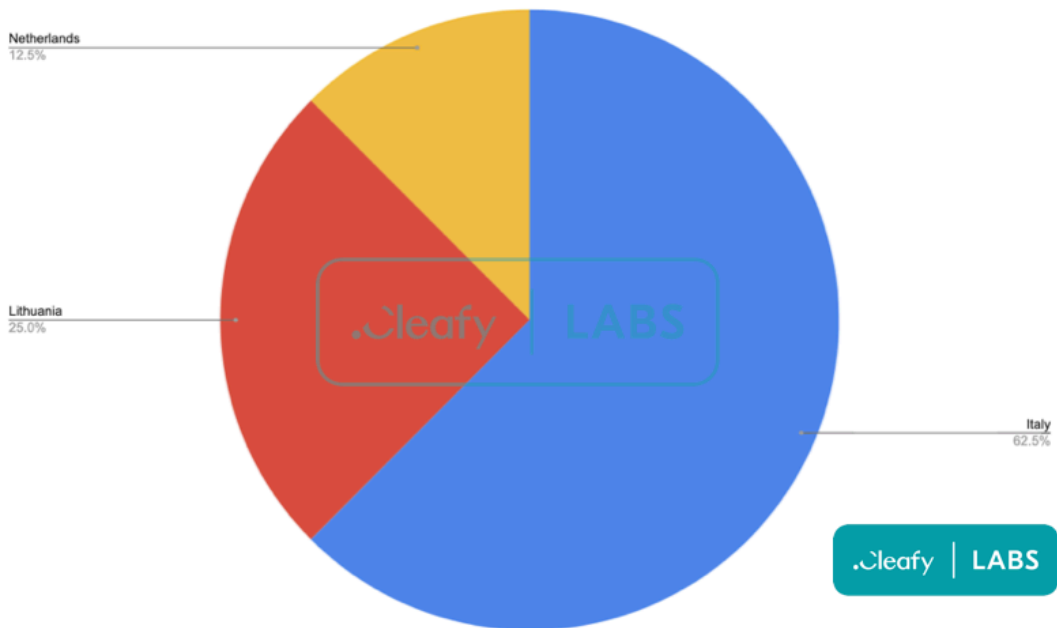


Figure 12 - Distribution of mule used by BRATA campaign

[1] TAs used a legitimate open source project (<https://github.com/serbanghita/Mobile-Detect>) to detect if the website is opened with a mobile phone or a PC.

BRATA main functionalities and capabilities

By analyzing the code of the malicious apps, it was possible to trace back the threat to the BRATA malware, a Brazilian malware discovered in 2019. However, these new samples present multiple differences compared to the previous one.

Several Portuguese/Brazilian logs embedded in the malicious app are shown to the victim in Italian. Our assumption is that, perhaps, the group responsible for maintaining the BRATA codebase, probably located in the LATAM area, is reselling this malware to other local groups. As a result, this threat is gradually expanding in several European countries.

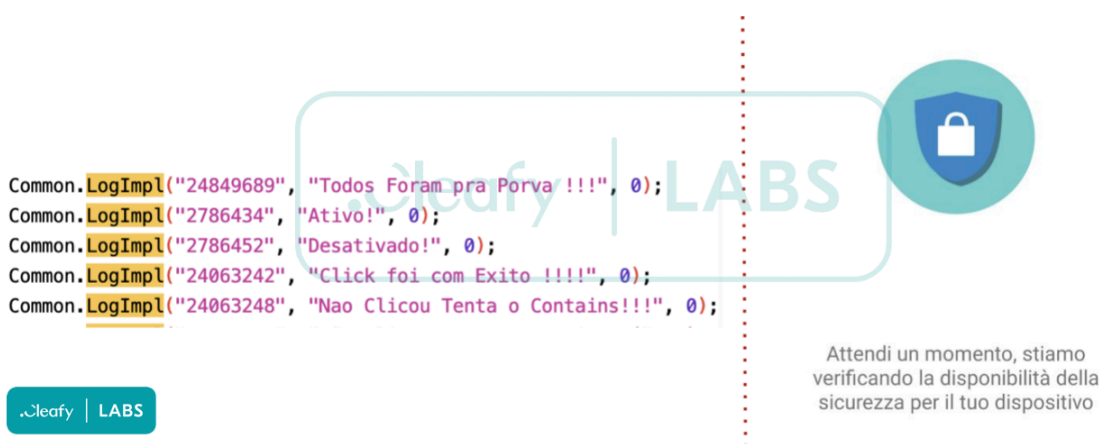


Figure 13 - Some BRATA logs (on the left) and a screen with Italian text (on the right)

Like other Android bankers previously appeared online (e.g., Teabot[2], Alien, Oscorp[3], etc.), this version of BRATA has RAT capabilities. The main difference resides in the implementation used to develop the malware: TAs used the b4a framework[4], already used by another Brazilian banker in 2019, called BasBanker. One of the reasons behind this choice is the possibility to import modules already designed by other developers. This characteristic may allow the TAs to speed up the implementation of new features or the malware itself.

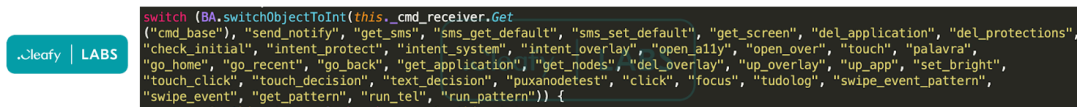


Figure 14 - List of commands used by BRATA malware

The main functionalities of this new version of BRATA are not very different from other “famous” banking trojan:

- Intercept SMS messages and forward them to a C2 server. This feature is used to get 2FA sent by the bank via SMS during the login phase or to confirm money transactions.
- Screen recording and casting capabilities that allow the malware to capture any sensitive information displayed on the screen. This includes audio, passwords, payment information, photo, and messages (as shown in Figure 15). Through the Accessibility Service, the malware clicks the “start now” button (of the popup) automatically, so the victim is not able to deny the recording/casting of the owned device.
- Remove itself from the compromised device to reduce detection.
- Uninstall specific applications (e.g., antivirus).
- Hide its own icon app to be less traceable by not advanced users.
- Disable Google Play Protect to avoid being flagged by Google as suspicious app.
- Modify the device settings to get more privileges.
- Unlock the device if it is locked with a secret pin or pattern.
- Show phishing page.
- Abuse the accessibility service to read everything that is shown on the screen of the infected device or to simulate click on the screen. This information is then sent to the C2 server of the attackers.

[2] <https://www.cleafy.com/cleafy-labs/teabot>

[3] <https://www.cleafy.com/cleafy-labs/ubel-oscorp-evolution>

[4] <https://www.b4x.com/b4a.html>

Conclusion

The Android Banking Trojan **BRATA** is already classified and blacklisted in our Threat Intelligence data with the following tags:

- ASK_BANKER_ANDROID_BRATA_V1
- ASK_BANKER_ANDROID_BRATA_V2

Appendix 1: IOCs

First campaign (June-mid September)

MD5	App Name	Package Name
ed63a9c22b2a6d39f11dfcee8925d306	Sicurezza Dispositivo	b4a.example
3cd6c14061a891c4a1525ac1a4609137	AntiSpam	com.dasjn023.dmindnasiod

Second campaign (October)

MD5	App Name	Package Name
8a10f6600be239a246e93cca0e7a69b0	Sicurezza Avanzata	com.voip.ffnenne

URL	Description
23.254.228.221:17178	BRATA C2
https[:]//bpweb-passadore[.]com	URL used to distribute the malicious app

Source: <https://www.cleafy.com/cleafy-labs/mobile-banking-fraud-brata-strikes-again>