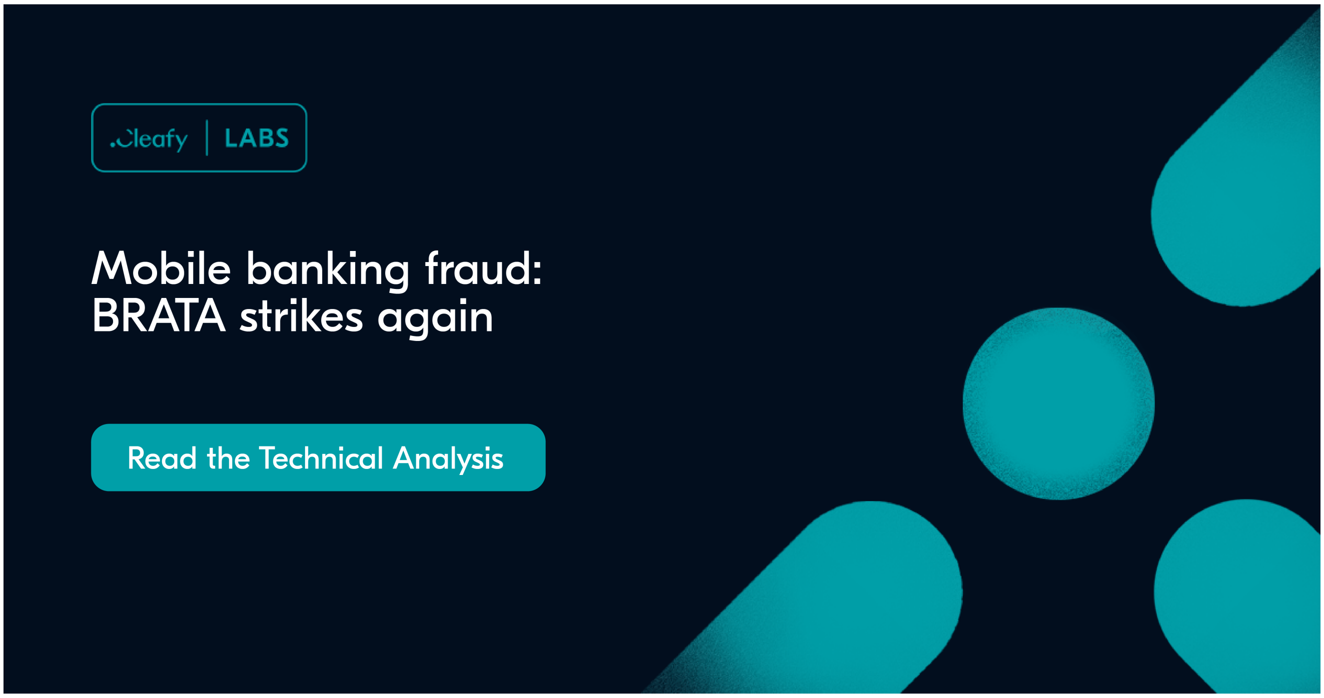
Mobile banking fraud: BRATA strikes again

cleafy.com/cleafy-labs/mobile-banking-fraud-brata-strikes-again

Federica Abbinante, Francesco Iubatti



Download your PDF guide to TeaBot

Get your free copy to your inbox now

Download PDF Version

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.

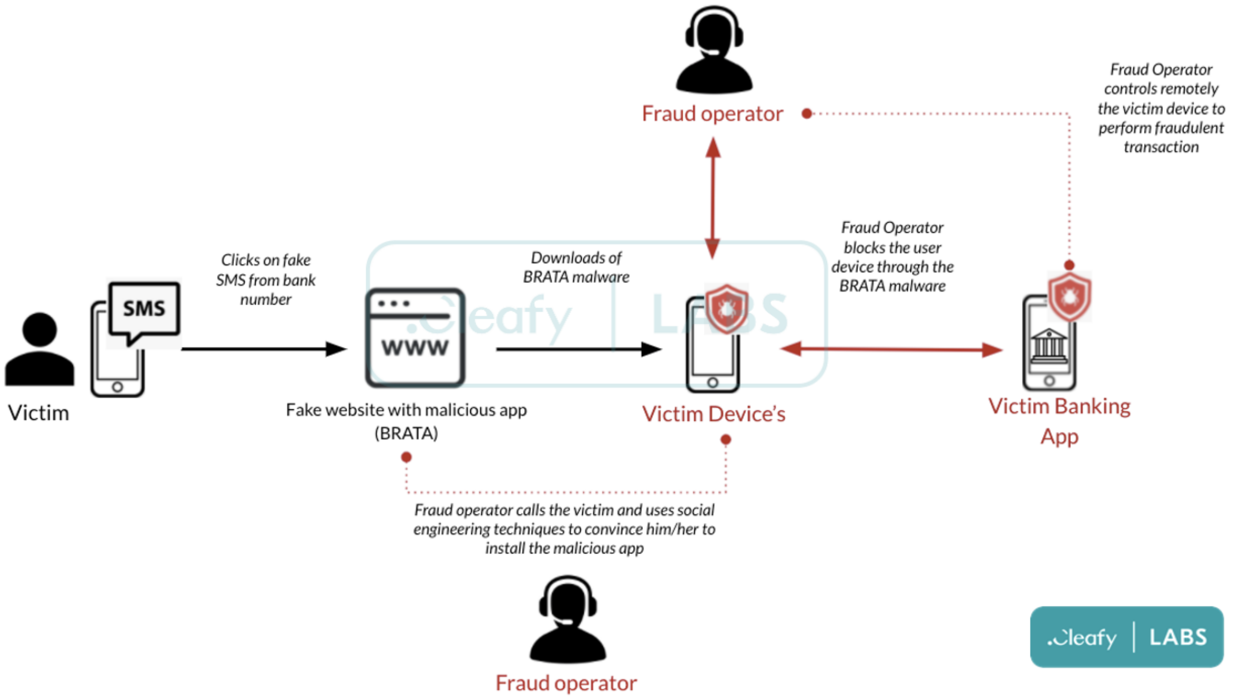
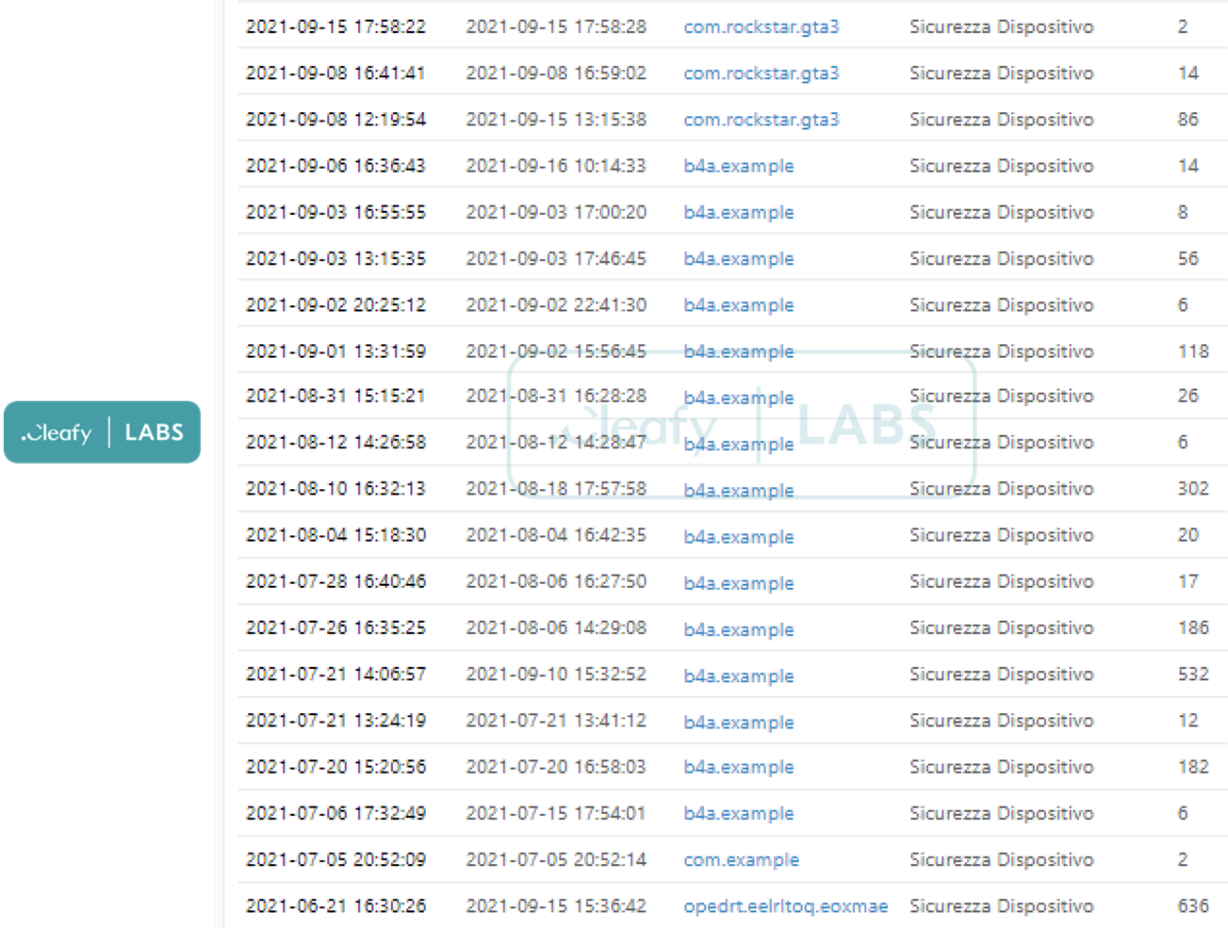

Fraud operator
Fraud Operator controls remotely the victim device to perform fraudulent transaction
Fraud Operator blocks the user device through the BRATA malware
Clicks on fake SMS from bank number
SMS
Downloads of BRATA malware
WWW
Victim
Fake website with malicious app (BRATA)
Victim Device's
Victim Banking App
Fraud operator calls the victim and uses social engineering techniques to convince him/her to install the malicious app
Fraud operator
.Cleafy | LABS

Figure 1 - BRATA distribution and modus operandi

Introduction

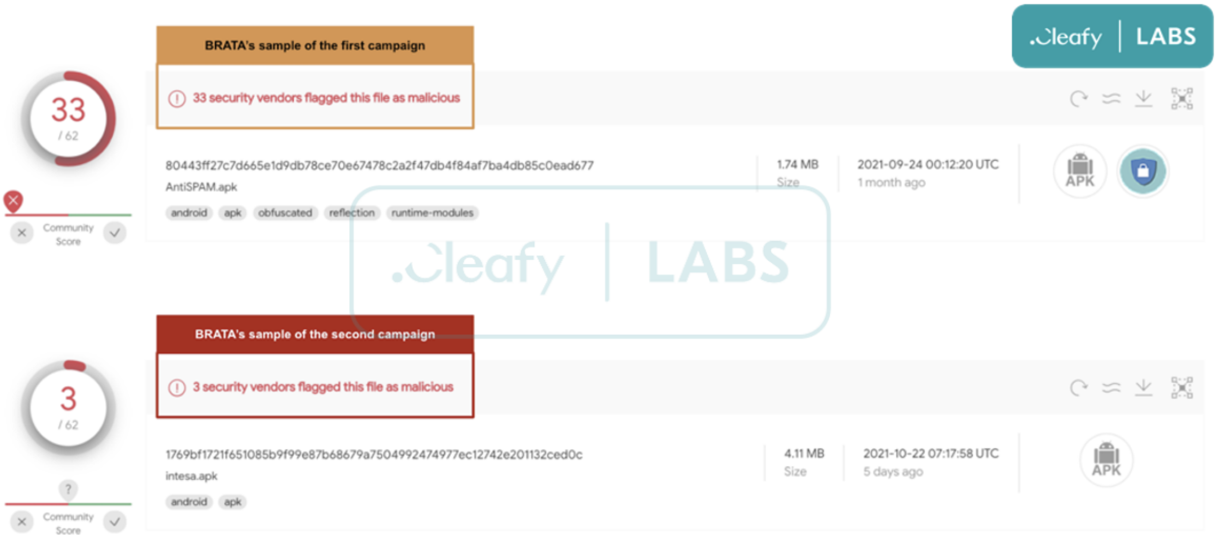
At the end of June 2021, the Cleafy Threat Intelligence and Incident Response team intercepted for the first time a new aggressive smishing campaign that was delivering multiple fake applications called “**Sicurezza Dispositivo**" (or “**AntiSPAM**”'). The campaign targeted the customers of one of the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



BRATA's sample of the first campaign

33 / 62

33 security vendors flagged this file as malicious

80443ff27c7d665e1d9db78ce70e67478c2a2f47db4f84af7ba4db85c0ead677
AntiSPAM.apk

android apk obfuscated reflection runtime-modules

1.74 MB Size

2021-09-24 00:12:20 UTC
1 month ago

BRATA's sample of the second campaign

3 / 62

3 security vendors flagged this file as malicious

1769bf1721f651085b9f99e87b68679a7504992474977ec12742e201132ced0c
intesa.apk

android apk

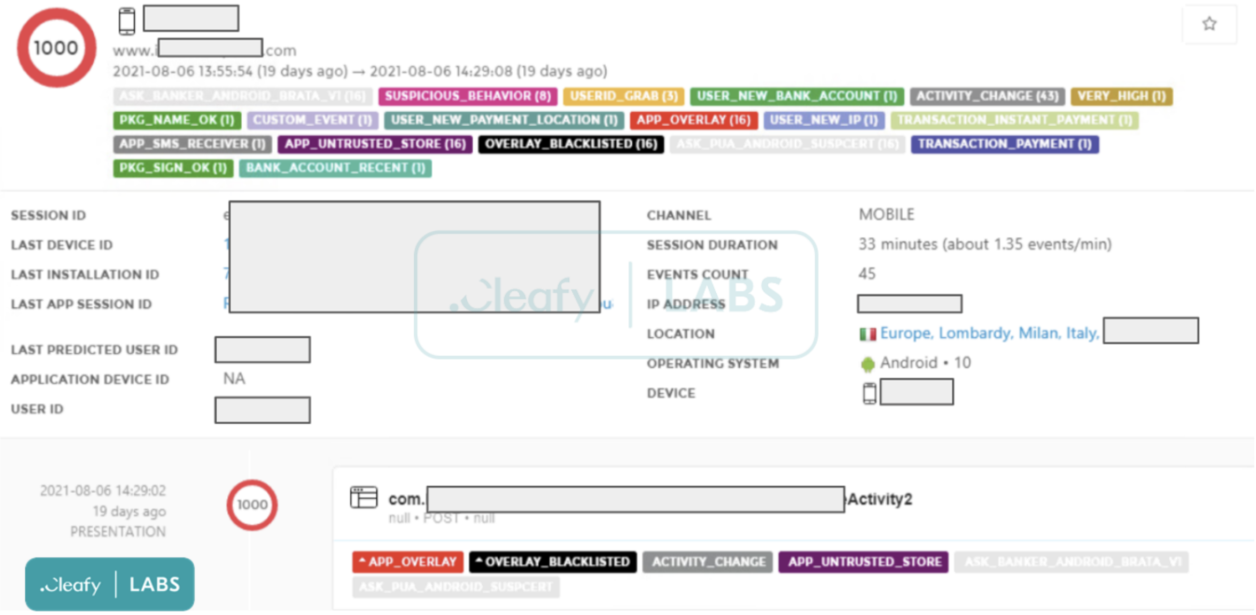
4.11 MB Size

2021-10-22 07:17:58 UTC
5 days ago

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.



1000 [redacted]
www.[redacted].com
2021-08-06 13:55:54 (19 days ago) → 2021-08-06 14:29:08 (19 days ago)

ASK_BANKER_ANDROID_BRATA_VI (16) SUSPICIOUS_BEHAVIOR (8) USERID_GRAB (3) USER_NEW_BANK_ACCOUNT (1) ACTIVITY_CHANGE (43) VERY_HIGH (1) PKG_NAME_OK (1) CUSTOM_EVENT (1) USER_NEW_PAYMENT_LOCATION (1) APP_OVERLAY (16) USER_NEW_IP (1) TRANSACTION_INSTANT_PAYMENT (1) APP_SMS_RECEIVER (1) APP_UNTRUSTED_STORE (16) OVERLAY_BLACKLISTED (16) ASK_PUA_ANDROID_SUSPCERT (16) TRANSACTION_PAYMENT (1) PKG_SIGN_OK (1) BANK_ACCOUNT_RECENT (1)

SESSION ID	[redacted]	CHANNEL	MOBILE
LAST DEVICE ID		SESSION DURATION	33 minutes (about 1.35 events/min)
LAST INSTALLATION ID		EVENTS COUNT	45
LAST APP SESSION ID		IP ADDRESS	[redacted]
		LOCATION	Europe, Lombardy, Milan, Italy, [redacted]
LAST PREDICTED USER ID	[redacted]	OPERATING SYSTEM	Android • 10
APPLICATION DEVICE ID	NA	DEVICE	[redacted]
USER ID	[redacted]		

2021-08-06 14:29:02
19 days ago
PRESENTATION

1000

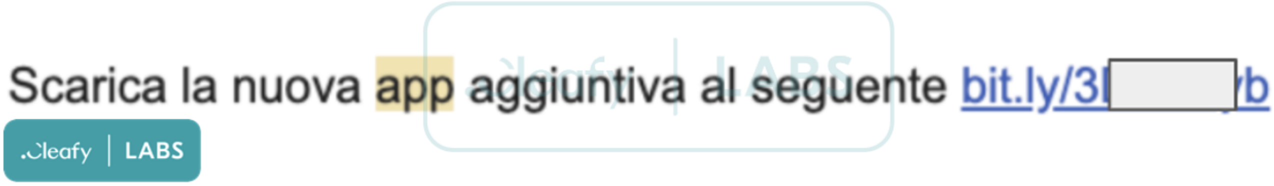
com.[redacted]Activity2
null • POST • null

APP_OVERLAY OVERLAY_BLACKLISTED ACTIVITY_CHANGE APP_UNTRUSTED_STORE ASK_BANKER_ANDROID_BRATA_VI ASK_PUA_ANDROID_SUSPCERT

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.

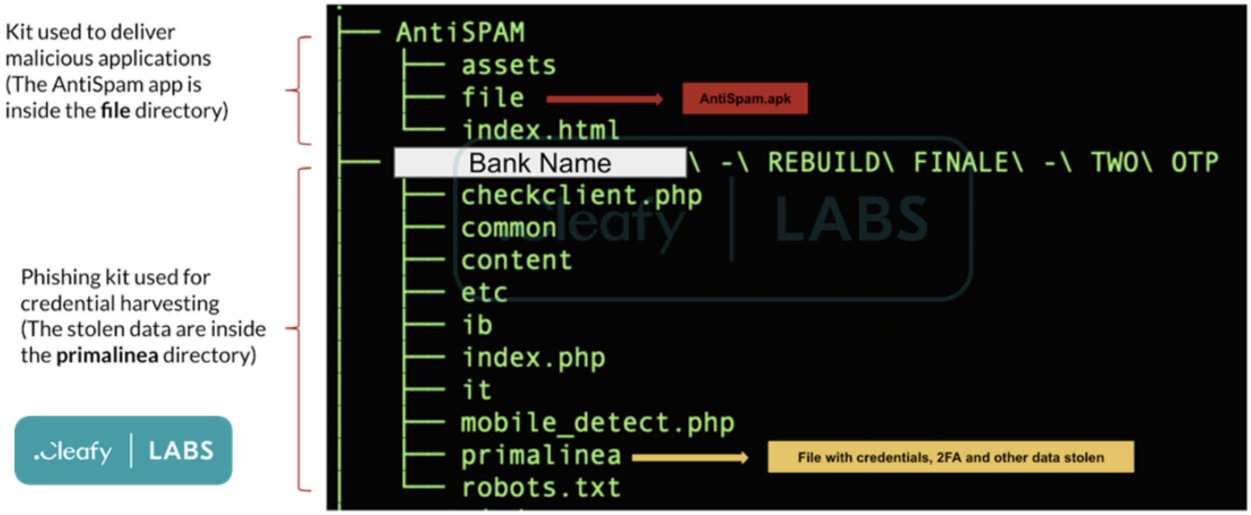
The attack chain usually starts with a fake SMS containing a link to a website. The SMS seems to come from the bank (the so-called spoofing scam), and it tries to convince the victim to download an anti-spam app, with the promise to be contacted soon by a bank operator.



Scarica la nuova app aggiuntiva al seguente bit.ly/3I[redacted]b

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).

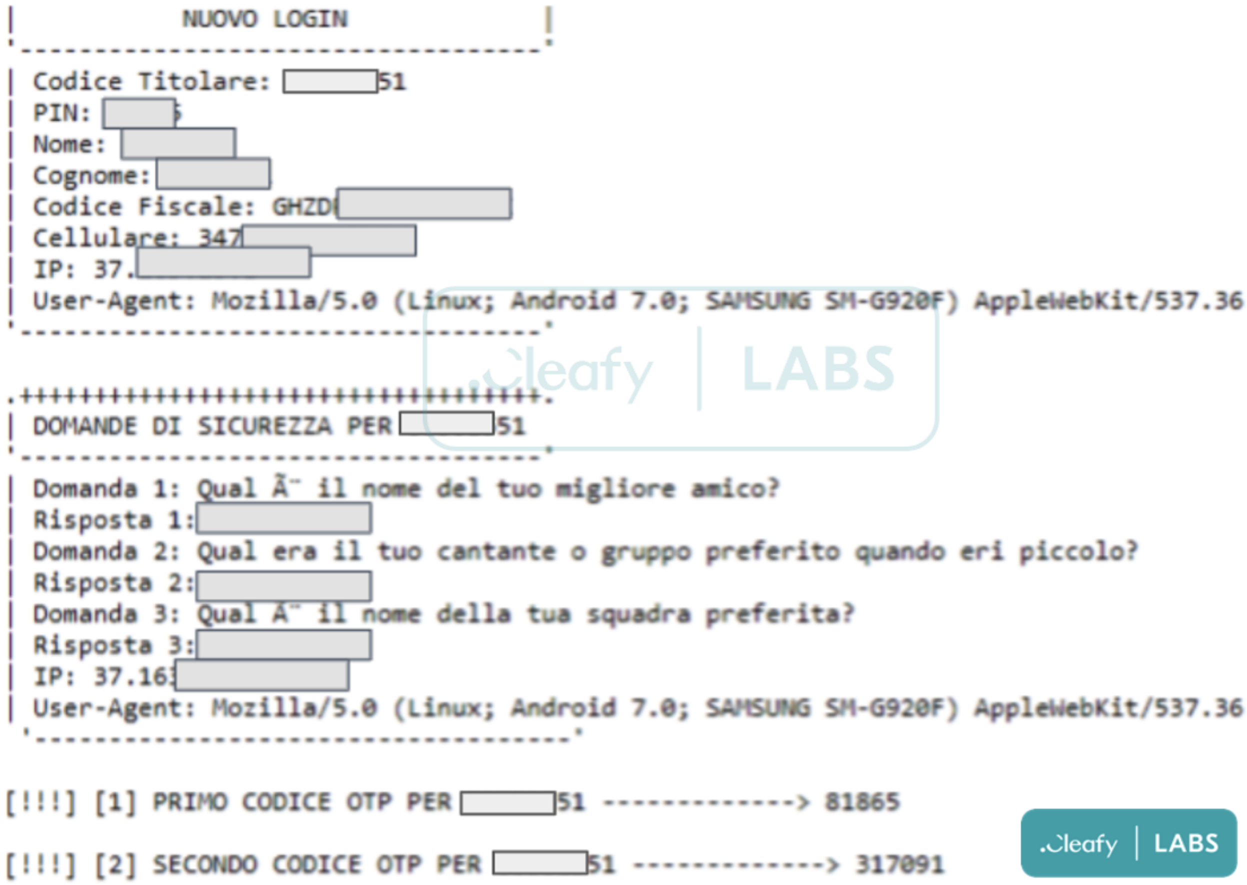


Kit used to deliver malicious applications (The AntiSpam app is inside the **file** directory)

Phishing kit used for credential harvesting (The stolen data are inside the **primalinea** directory)

```
├── AntiSPAM
│   ├── assets
│   ├── file
│   └── index.html
├── Bank Name\ -\ REBUILD\ FINALE\ -\ TWO\ OTP
│   ├── checkclient.php
│   ├── common
│   ├── content
│   ├── etc
│   ├── ib
│   ├── index.php
│   ├── it
│   ├── mobile_detect.php
│   ├── primalinea
│   └── robots.txt
```

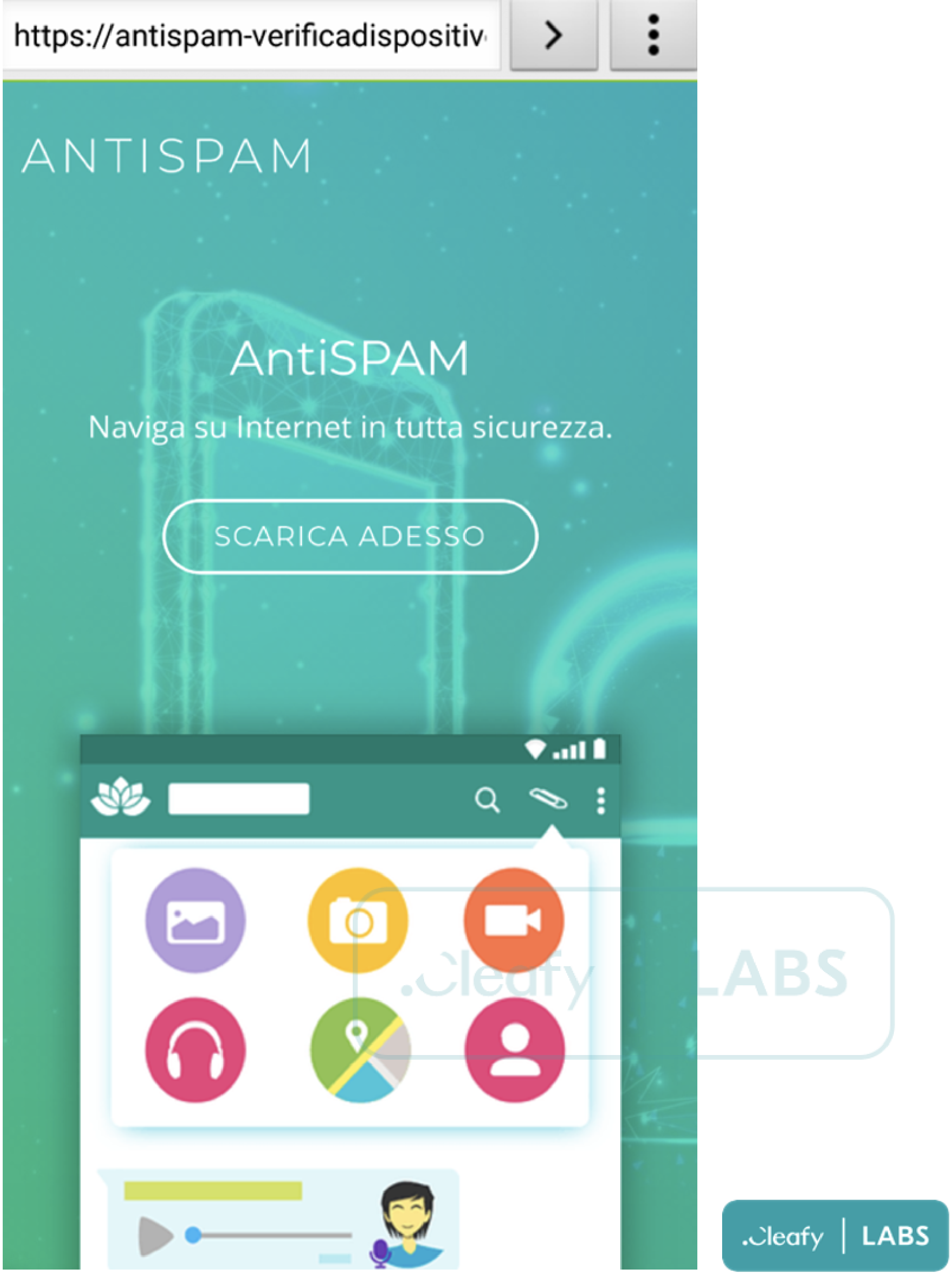
Figure 6 - Phishing kit used by TAs to deliver BRATA and for credential harvesting



```
|          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 Ã¨ 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 Ã¨ 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.



https://antispam-verificadispositiv

ANTISPAM

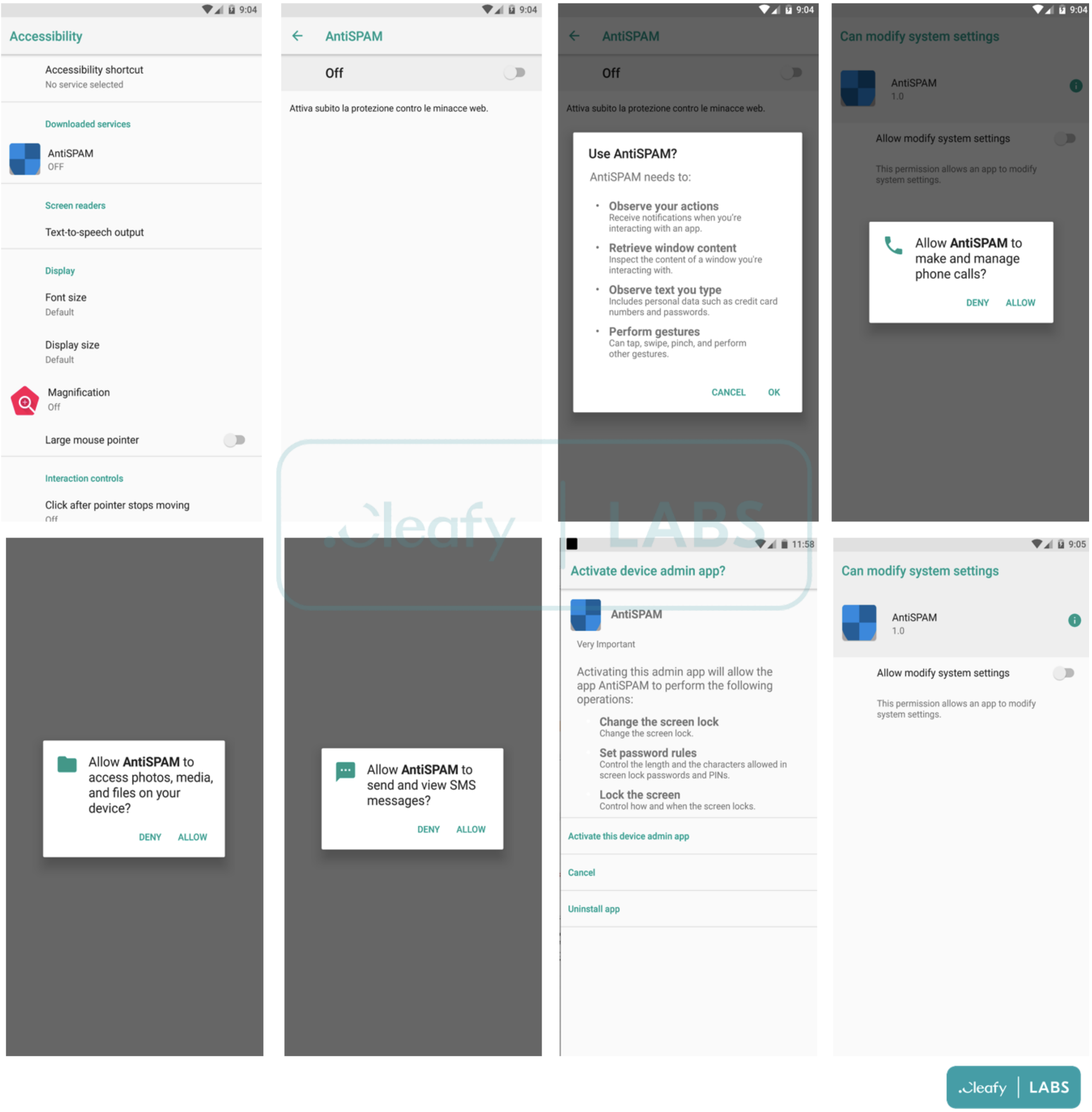
AntiSPAM

Naviga su Internet in tutta sicurezza.

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.



Accessibility

Accessibility shortcut
No service selected

Downloaded services

AntiSPAM
OFF

Screen readers

Text-to-speech output

Display

Font size
Default

Display size
Default

Magnification
Off

Large mouse pointer

Interaction controls

Click after pointer stops moving
Off

AntiSPAM

Off

Attiva subito la protezione contro le minacce web.

AntiSPAM

Off

Attiva subito la protezione contro le minacce web.

Use AntiSPAM?

AntiSPAM needs to:

- Observe your actions
  Receive notifications when you're interacting with an app.
- Retrieve window content
  Inspect the content of a window you're interacting with.
- Observe text you type
  Includes personal data such as credit card numbers and passwords.
- Perform gestures
  Can tap, swipe, pinch, and perform other gestures.

CANCEL OK

Can modify system settings

AntiSPAM
1.0

Allow modify system settings

This permission allows an app to modify system settings.

Allow **AntiSPAM** to make and manage phone calls?

DENY ALLOW

Allow **AntiSPAM** to access photos, media, and files on your device?

DENY ALLOW

Allow **AntiSPAM** to send and view SMS messages?

DENY ALLOW

Activate device admin app?

AntiSPAM

Very Important

Activating this admin app will allow the app AntiSPAM to perform the following operations:

Change the screen lock
Change the screen lock.

Set password rules
Control the length and the characters allowed in screen lock passwords and PINs.

Lock the screen
Control how and when the screen locks.

Activate this device admin app

Cancel

Uninstall app

Can modify system settings

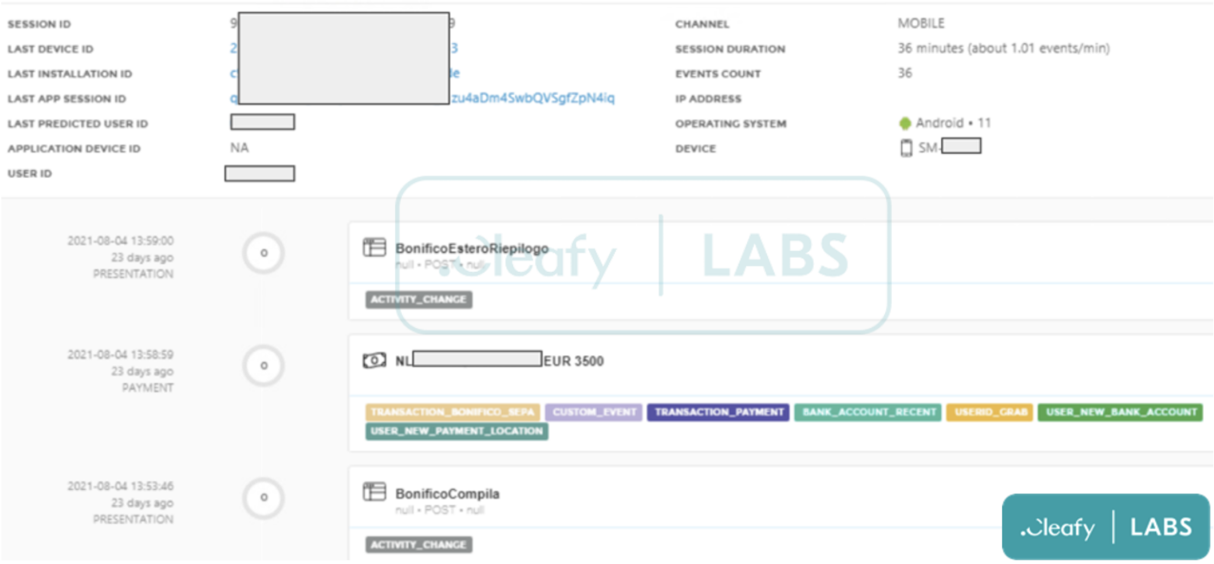
AntiSPAM
1.0

Allow modify system settings

This permission allows an app to modify system settings.

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.



SESSION ID	9[redacted]9	CHANNEL	MOBILE
LAST DEVICE ID	2[redacted]3	SESSION DURATION	36 minutes (about 1.01 events/min)
LAST INSTALLATION ID	c[redacted]le	EVENTS COUNT	36
LAST APP SESSION ID	q[redacted]zu4aDm4SwbQVSgfZpN4iq	IP ADDRESS	
LAST PREDICTED USER ID	[redacted]	OPERATING SYSTEM	Android • 11
APPLICATION DEVICE ID	NA	DEVICE	SM-[redacted]
USER ID	[redacted]		

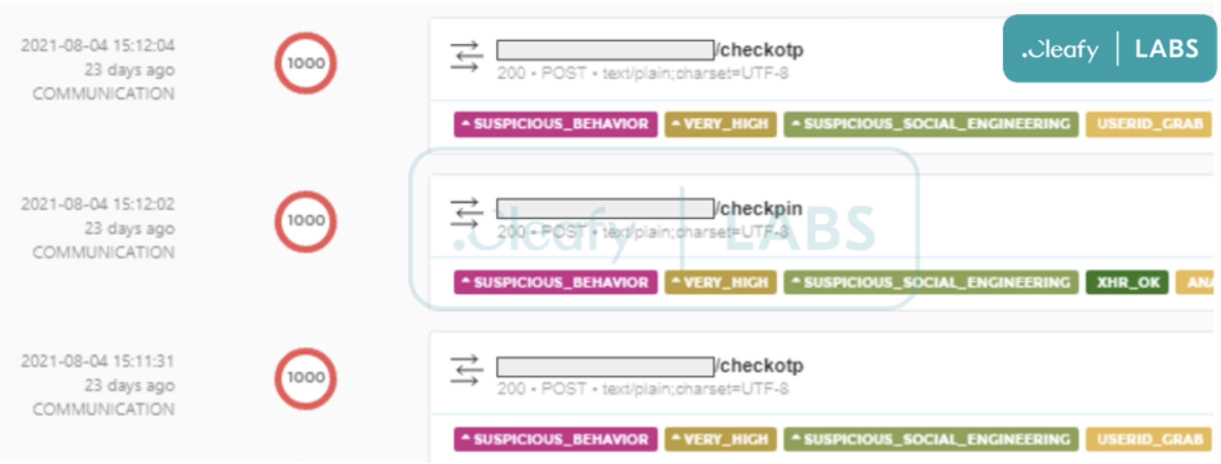
2021-08-04 13:59:00
23 days ago
PRESENTATION
0
BonificoEsteroRiepilogo
null • POST • null
ACTIVITY_CHANGE

2021-08-04 13:58:59
23 days ago
PAYMENT
0
NL[redacted]EUR 3500
TRANSACTION_BONIFICO_SEPA CUSTOM_EVENT TRANSACTION_PAYMENT BANK_ACCOUNT_RECENT USERID_GRAB USER_NEW_BANK_ACCOUNT USER_NEW_PAYMENT_LOCATION

2021-08-04 13:53:46
23 days ago
PRESENTATION
0
BonificoCompila
null • POST • null
ACTIVITY_CHANGE

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.



2021-08-04 15:12:04
23 days ago
COMMUNICATION
1000
[redacted]/checkotp
200 • POST • text/plain;charset=UTF-8
SUSPICIOUS_BEHAVIOR VERY_HIGH SUSPICIOUS_SOCIAL_ENGINEERING USERID_GRAB

2021-08-04 15:12:02
23 days ago
COMMUNICATION
1000
[redacted]/checkpin
200 • POST • text/plain;charset=UTF-8
SUSPICIOUS_BEHAVIOR VERY_HIGH SUSPICIOUS_SOCIAL_ENGINEERING XHR_OK AN

2021-08-04 15:11:31
23 days ago
COMMUNICATION
1000
[redacted]/checkotp
200 • POST • text/plain;charset=UTF-8
SUSPICIOUS_BEHAVIOR VERY_HIGH SUSPICIOUS_SOCIAL_ENGINEERING USERID_GRAB

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.

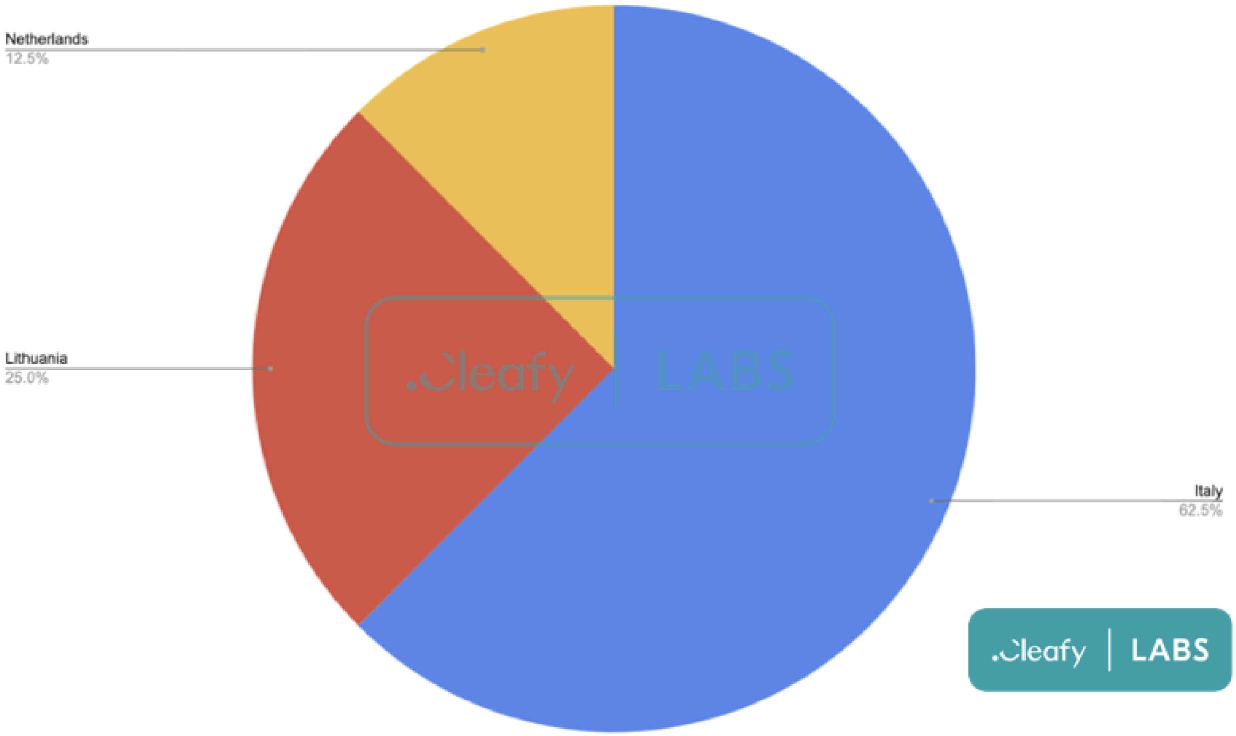
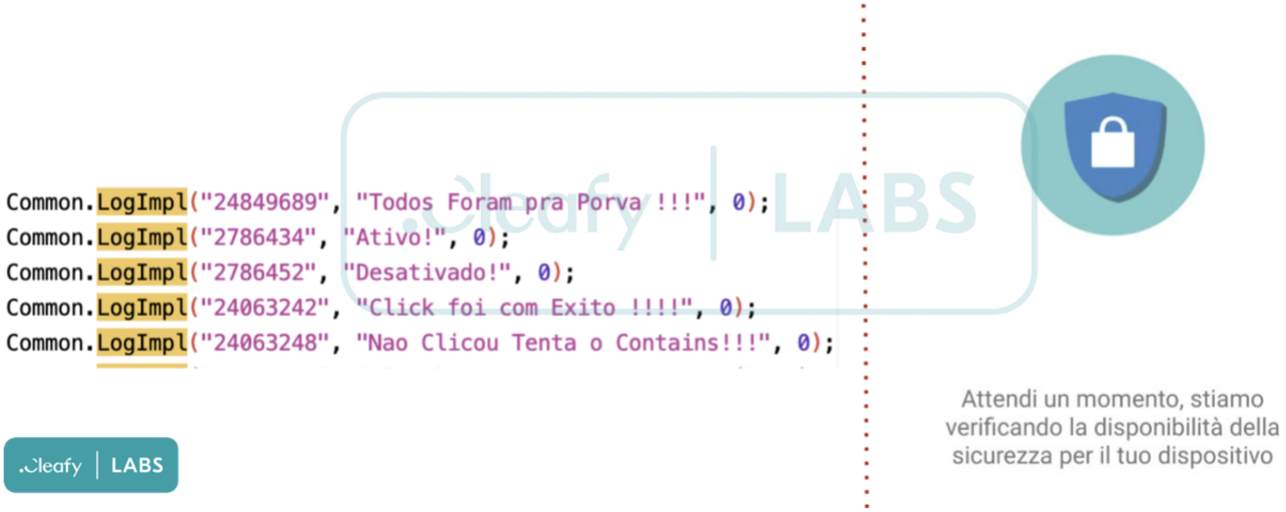


Figure 12 - Distribution of mule used by BRATA campaign
[1] TAs used a legitimate open source project (https://github.com/serbanghita/Mobile-Detect) to detect if the website is opened with a mobile phone or a PC.

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.

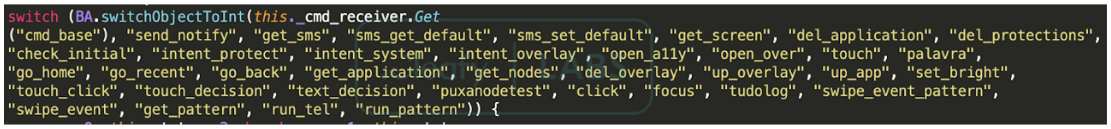


```
Common.LogImpl("24849689", "Todos Foram pra Porva !!!", 0);
Common.LogImpl("2786434", "Ativo!", 0);
Common.LogImpl("2786452", "Desativado!", 0);
Common.LogImpl("24063242", "Click foi com Exito !!!!", 0);
Common.LogImpl("24063248", "Nao Clicou Tenta o Contains!!!", 0);
```

Attendi un momento, stiamo verificando la disponibilità della sicurezza per il tuo dispositivo

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.



```
switch (BA.switchObjectToInt(this._cmd_receiver.Get
("cmd_base"), "send_notify", "get_sms", "sms_get_default", "sms_set_default", "get_screen", "del_application", "del_protections",
"check_initial", "intent_protect", "intent_system", "intent_overlay", "open_a11y", "open_over", "touch", "palavra",
"go_home", "go_recent", "go_back", "get_application", "get_nodes", "del_overlay", "up_overlay", "up_app", "set_bright",
"touch_click", "touch_decision", "text_decision", "puxanodetest", "click", "focus", "tudolog", "swipe_event_pattern",
"swipe_event", "get_pattern", "run_tel", "run_pattern")) {
```

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