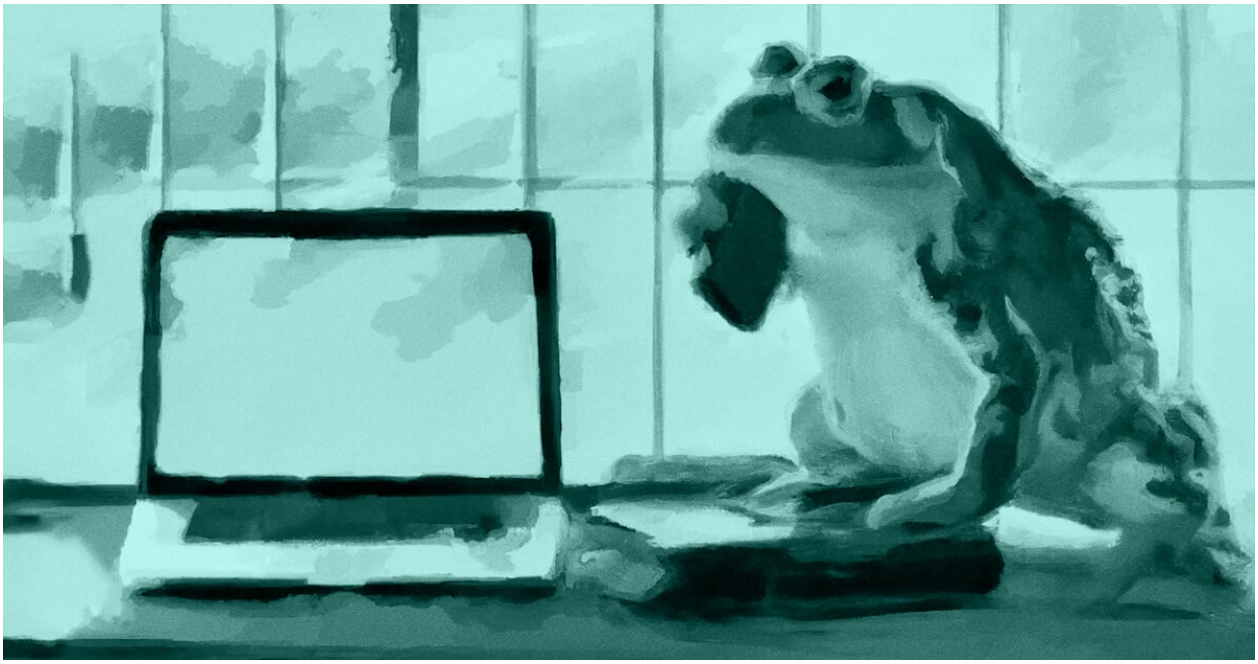
TOAD attacks: Vishing combined with Android banking malware now targeting Italian banks

threatfabric.com/blogs/toad-fraud



Jump to

Introduction

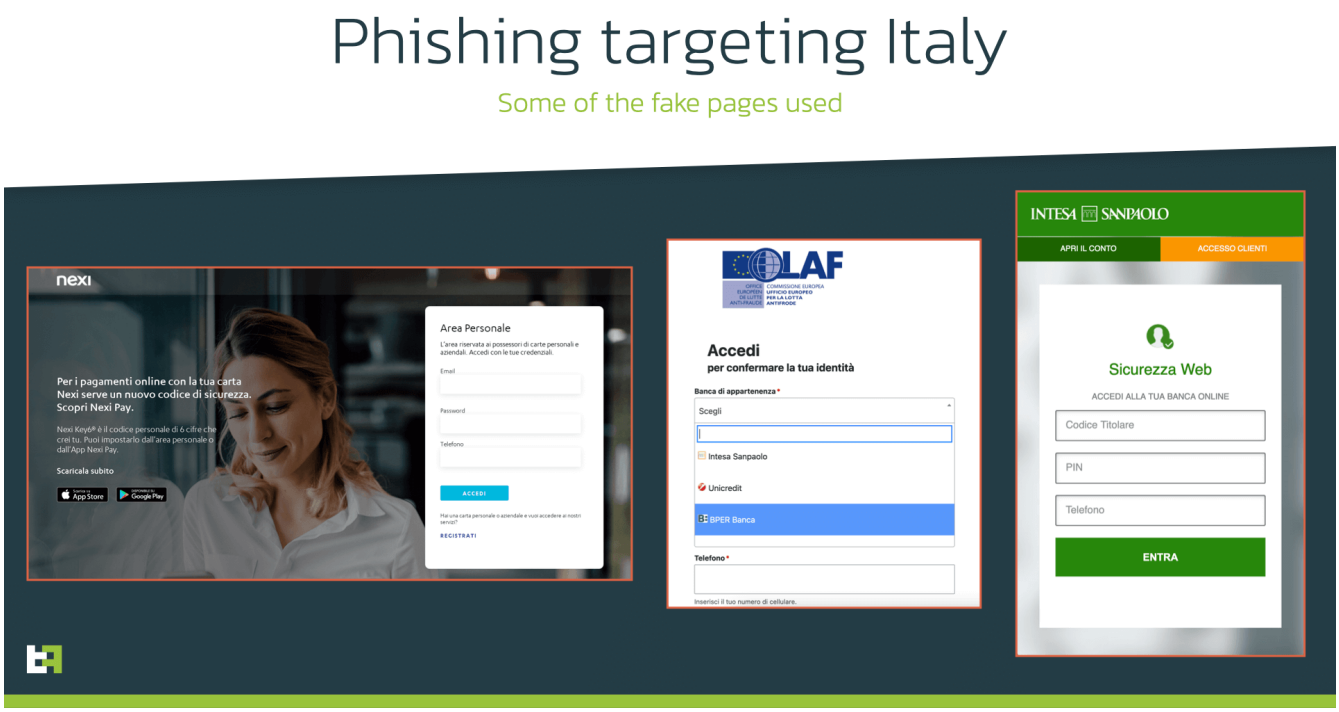
Our Threat Intelligence (TI) shows that telephone-oriented attack delivery (TOAD) tactics are becoming increasingly popular amongst fraudsters orchestrating Android banking malware campaigns. Recently, such case was reported targeting customers of an Indian bank as spotted by MalwareHunterTeam.

During one of our latest investigations, ThreatFabric's analysts uncovered a network of phishing websites targeting Italian online-banking users and aiming to steal their banking credentials. Further research defined a connection between this network and the Android banking Trojan dubbed Copybara, that is involved in telephone-oriented attack delivery performed by the threat actors. Latest version of it introduced unique feature that allows to build and show dynamic fake forms on the fly. With the increase in popularity of voice phishing

(vishing) attacks, where criminals coach victims into installing Android banking malware, we are entering a new era of hybrid fraud attacks. Despite the popularity of this technique, and the clear trend based on campaigns discovered, vishing used as malware distribution tactic is currently not covered by MITRE mobile matrix.

Discovered campaign targeting Italy

The campaign discovered by our analysts is targeting multiple Italian banks and their customers. It involves multiple phishing sites impersonating several Italian financial services and anti-fraud offices, as it can be seen on the following screenshots:



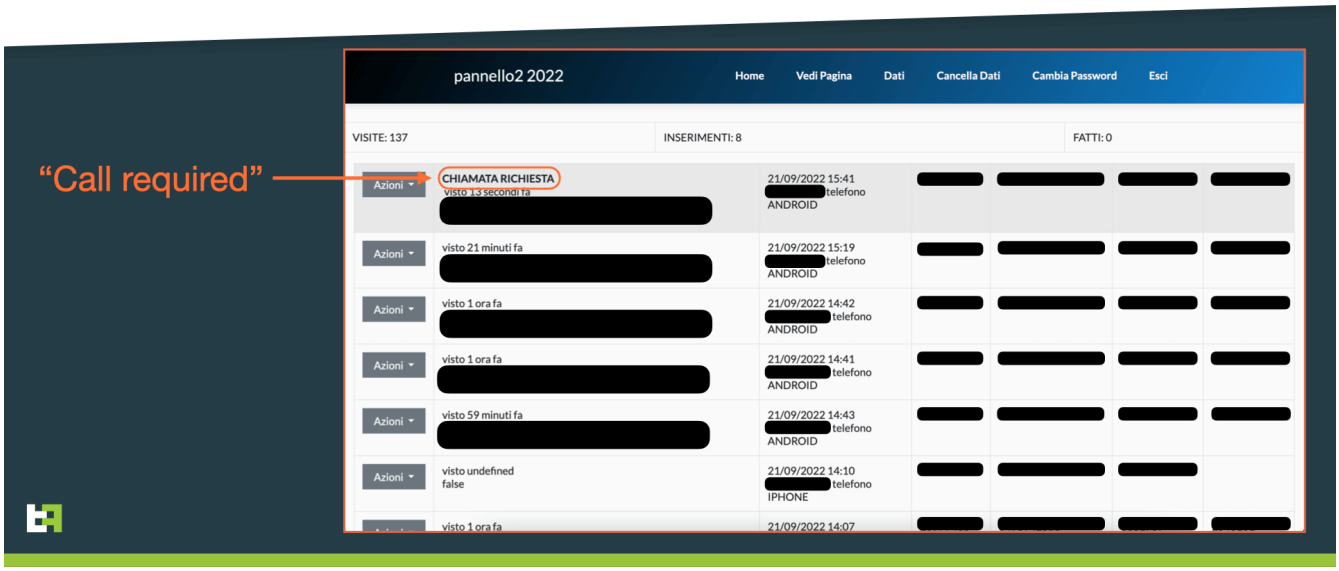
To maintain and manage the large number of phishing pages used in these campaigns, the threat actor(s) used several phishing kits that are quite well-known in the underground scene. Such kits allow to easily create the phishing page, automatically register phishing domain names and create a short link for it to be used in distribution. Besides, they also provide a panel that allows to maintain all created websites and monitor their activity. Such panel is also provided as a service by one of the cybercriminal groups on the underground forum.

All phishing sites seen in the campaign request similar set of personal data: account number, PIN code, telephone number. Our team noticed that, in some cases, cybercriminals request victims to choose secret questions and answers that were set during the registration process with the bank as second factor of authentication. Obviously, collecting this data can help cybercriminals to get access to victim's banking accounts.

After submitting the data, victims are notified that a support operator will contact them soon (using the previously collected phone number). At this point, the next step of the campaign takes place: the installation of Android banking Trojan, with the help of the operator, as part of telephone-oriented attack delivery (TOAD). The threat actor calls victims and gives instructions to install the necessary "security" app on victim's device.

Phishing kit control panel

Stolen data (clients' IDs, PIN codes, phone numbers)

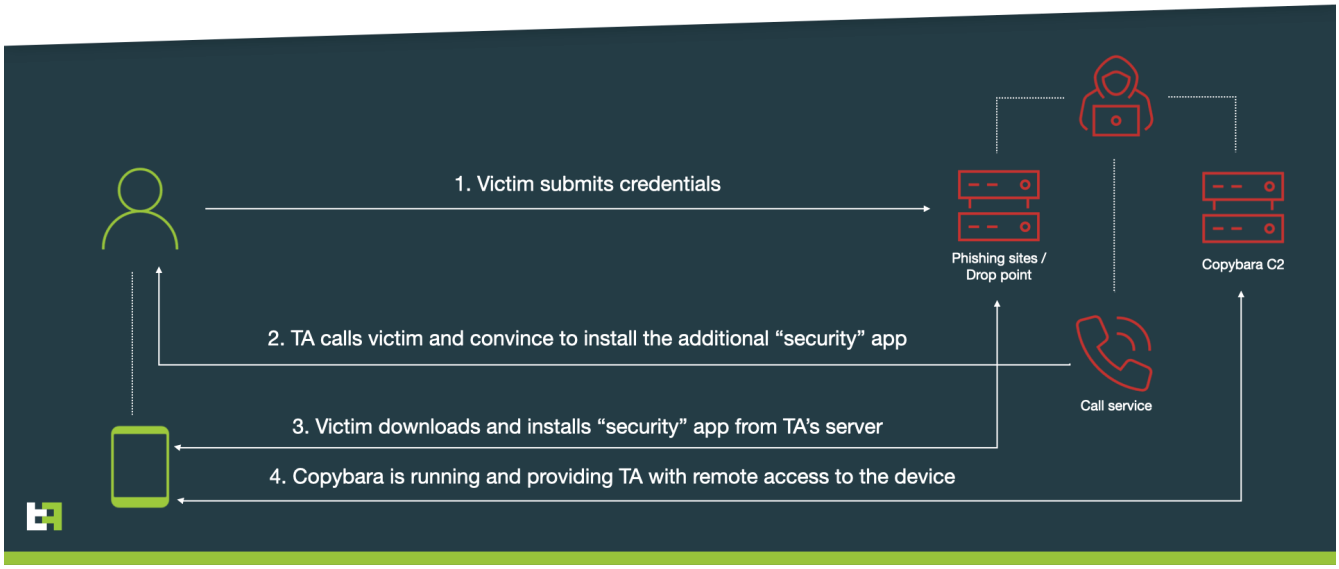


Telephone-oriented attack delivery threats involve direct call between cybercriminals (e.g., malicious call center) and a victim. During this call, the victim is being convinced and instructed to install some additional software on his/her devices in order for threat actor to be able to perform some further fraud. The installed software can be legitimate remote access tools that are used by cybercriminals to have a remote control over victim's device.

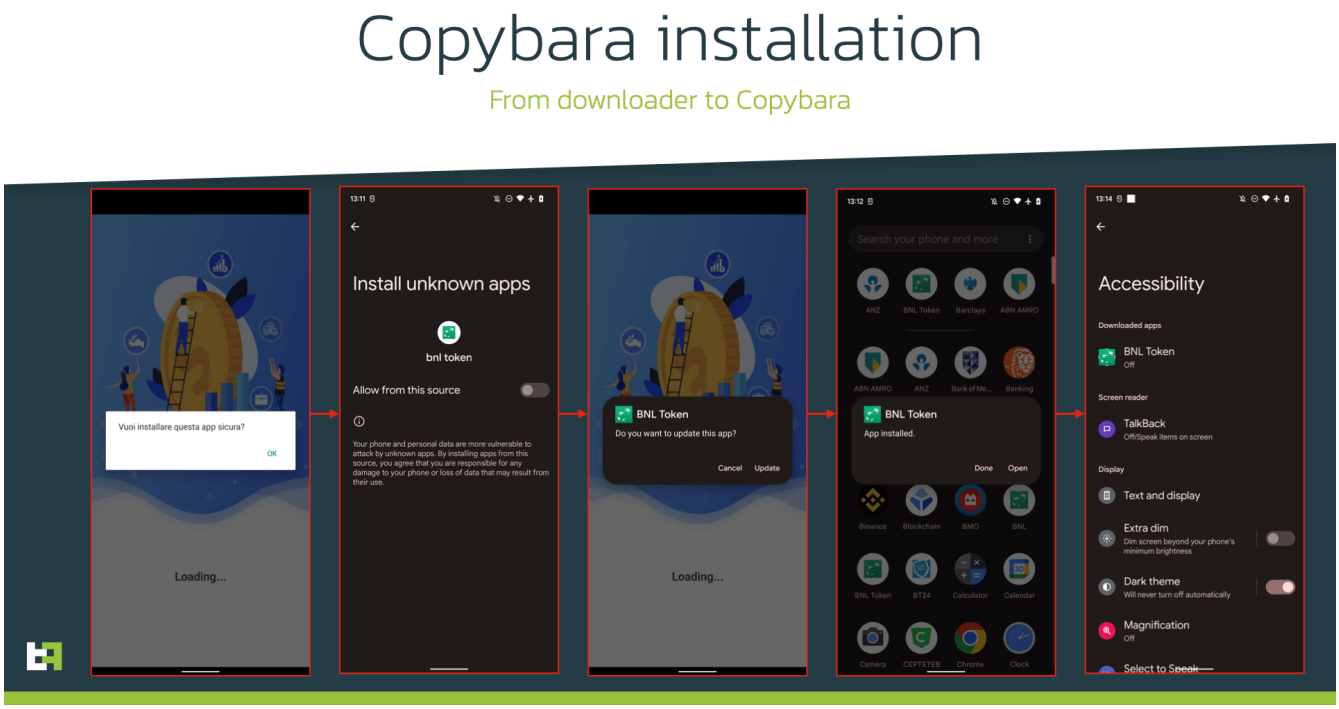
However, in some cases the victim is instructed to download and install some specific malicious software developed or maintained by threat actors. This is the case for the campaign discovered by ThreatFabric analysts, which involves both phishing sites and subsequent TOAD with installation of Copybara Android banking Trojan.

Telephone-oriented attack delivery

Copybara case



As an entry point for cybercriminals, the victim is asked to install a downloader app that will download the actual payload. The payload then is installed as an update for the downloader, substituting it.



However, the “security” app that is installed on the device is an Android Trojan, that ThreatFabric is tracking as Copybara. This malware family is also referred to as BRATA by some researchers. However, our threat intelligence shows that it is not related to original BRATA reported back in 2019 targeting Brazilian users. We uncovered differences between multiple families named BRATA in our blog.

Our research also reveals the name of the threat used by the TAs: **Joker**. Coincidentally, this name is also used by another Android malware family, usually distributed through Google Play, and which specializes in personal information stealing and Subscription services fraud. ThreatFabric can confirm that there is no connection with this malware family and the one discussed in this blogpost, distributed via TOAD. To avoid confusion, we will refer to this new malware family with the initial name that we assigned to it upon discovery, which is Copybara.

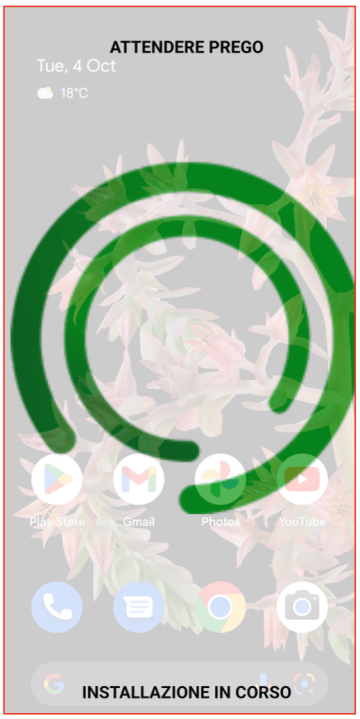
Copybara: Ctrl+C, Ctrl+V, innovations

First samples of Copybara seen by ThreatFabric date back to November, 2021. Despite the fact that it was referred as BRATA by other researchers, TF analysts were able to clearly define it as a separate family, despite using the same framework for development. The name “Copybara” was given by our malware analysts is reference to TAs development process: Copybara’s code has a lot of parts directly copied and pasted from other publicly available modules. Sometimes (like for example with Copybara’s downloader) the code is taken as-is with minor changes in variables.

However, such approach does not directly imply the weakness of the malware. Despite the code being messy and full of non-active sections, the TAs managed to equip the Trojan with remote access capability, which tries to masquerade itself as security udpate, while the criminals are performing actions on the infected device “behind the curtains”. While the TA is connected to infected device, Copybara shows a fake overlay that is semi-transparent to cover the actions of the cyber criminals.

Fake overlay

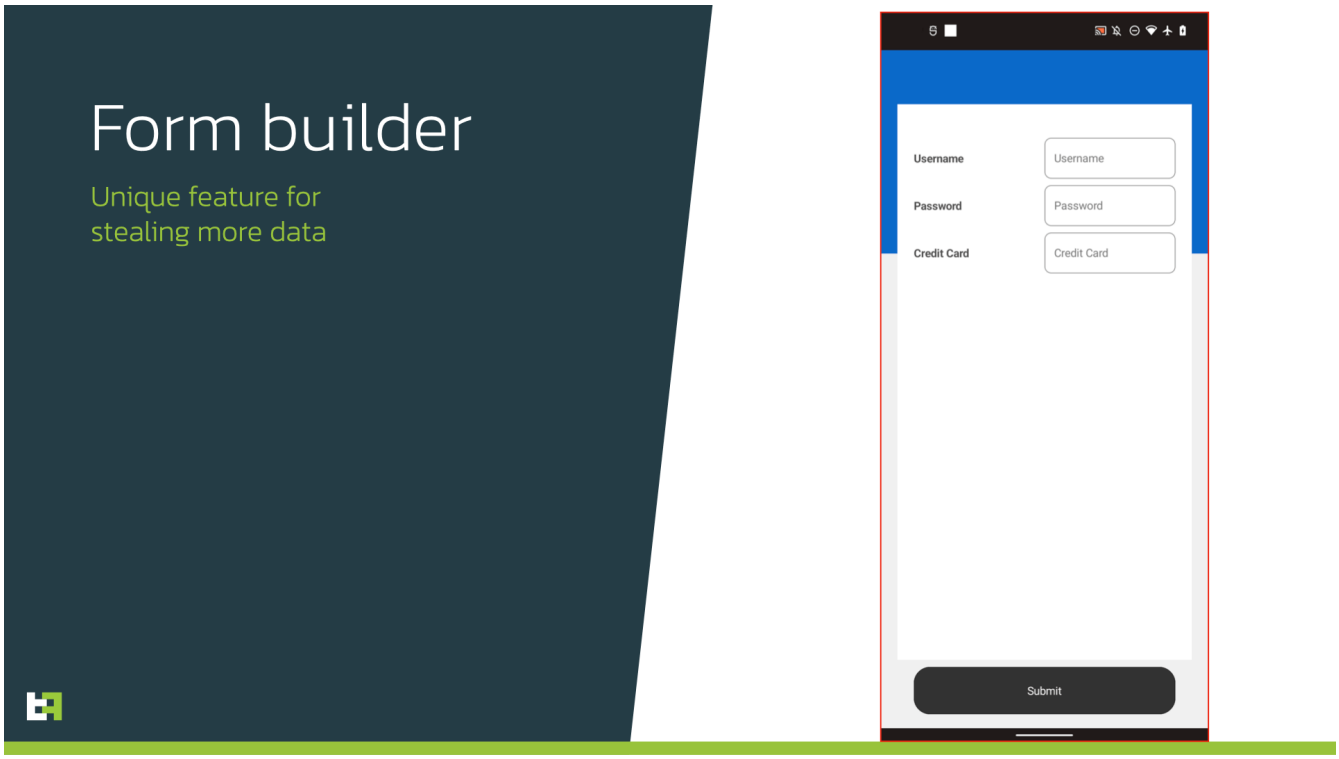
Hiding fraudulent activity



It allows actors to stay low and not drag attention of the victim while performing fraudulent actions within the banking applications, using data previously stolen with phishing. Copybara's RAT capabilities are powered by abusing the AccessibilityService: the C2 server sends a specific command/action to perform and Copybara handles it with the help of its Accessibility engine. TAs can open arbitrary apps, install additional ones, perform clicks and swipes, enter text to the text fields, etc.

TF received reports that TA's use Copybara's ability to uninstall packages in order to remove the original banking app to leave the detection window as small as possible.

Another quite unique feature recently introduced by authors is the ability to dynamically build fake input forms and show it to victims. Actors are able to specify arbitrary input fields, text labels, check boxes and collect even more data from victims. At the moment these forms are quite simplistic, but the dynamic approach allows TAs to use full power of Android OS to build genuine-looking screens on-the-fly.



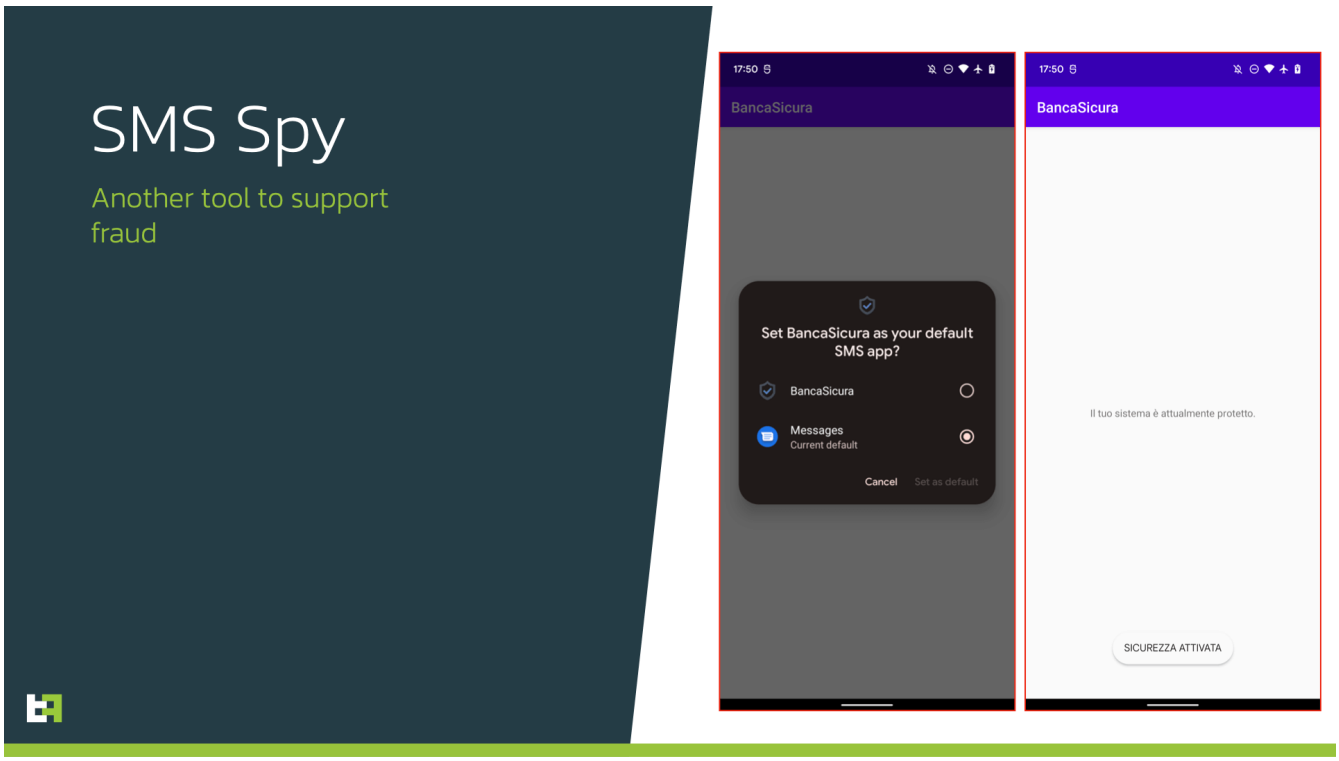
The full list of supported commands of Copybara is provided below.

Command	Description
SendMsg_changeloopsizefromadm	not used anymore
Send_OutgoingConnection	Initialize new remote connection
permclicked*	Initiate request for various permissions
clickondisableenablenoti	Open app notifications settings
getdevicecalllogs	Upload device contacts to the C2
SendMsg_SendCallDivert	Call to specified number
getdevicegpdata	Send device specific data
sendfaknotiinfo	Create a notification with specified title and text
wsh_setkeylogapp	Specify the target for keylogging
wsh_LoadKeyLogData	Upload keylogging data to the C2
SendMsg_ClickAddLockNewF	Display new overlay
SendMsg_ClickAddLockNewQRCode	Display new overlay
SendMsg_ClickBackButton	Perform click on “Back” button
SendMsg_ClickView	Perform click by coordinates
SendMsg_ClickSwipe	Perform swipe by coordinates
SendMsg_OpenApp	Start specified app
SendMsg_SendTextToView	Set specified text

Command	Description
SendMsg_SendTextToViewFromKey	Set specified text
SendMsg_RefreshData	Clear all notifications
SendMsg_ClickHomeButton	Perform click on “Home” button
SendMsg_ClickRemoveLock	Close overlay
SendMsg_DisconnectFromB4J	Close remote connection
SendMsg_OpenRecentApps	Open recent apps list
SendMsg_formatdevice	Perfom device formatting
SendMsg_sendmesc	Send screenshot to the C2
SendMsg_closescreenshot	Stop screencasting
SendMsg_ClickAddLock	Display overlay
SendMsg_StartScrl	Perform scroll
SendMsg_Uninstallapp	Uninstall specified app
SendMsg_UninstallThisapp	Uninstall itself
SendMsg_DeleteApp	Delete app from blocked list
SendMsg_Blockapp	Add app to blocked list
SendMsg_DialNumber	Call to specified number
buildtheform	Dynamically build the activity
SendMsg_USSDKeys	Open activity for USSD request
wsh_sendsmsmessages	Send SMS messages
SendMsg_SendSMSToNumber	Send SMS to specified number
wsh_WakeupPhone	“Wake up” the device by sending clicks
downinstappp	Download and install specified app

Not only Copybara

Further investigation of the infrastructure utilized by the threat actor(s) reveals certain interesting ties to other Trojans. One of the campaigns involved SMS stealing Trojan. This piece of malware is quite simple in its capabilities, only allowing the actors to get control over incoming messages: all the incoming SMS messages are uploaded to TAs server, thus allowing the TA to perform so-called “new device registration” fraud and log in with other channel (e.g. web) and intercept all OTPs sent by bank to validate login and further transactions.



Conclusion

Telephone-oriented attack delivery (TOAD) cases are becoming a trend on the current mobile threat landscape. Personal approach powered with social engineering techniques allow cybercriminals to trick unsuspicious victims and obtain installations of their Trojans with high likelyhood of success. Moreover, most of the cases end up installing some legitimate remote access tools that are not flagged/detected by antivirus engines.

We believe that such complicated cases involving threat actor - victim interaction should not be approached in a conventional, traditional way. Behaviour analytics powered by strong Threat Intelligence is a way to cope with such fraudulent activity as it provides additional indicators to detect suspicious activity.

Fraud Risk Suite

ThreatFabric's Fraud Risk Suite enables safe & frictionless online customer journeys by integrating industry-leading mobile threat intel, behavioural analytics, advanced device fingerprinting and over 10.000 adaptive fraud indicators. This will give you and your customers peace of mind in an age of ever-changing fraud.

Appendix

CopybaraDropper Samples

App name	Package name	SHA-256
iSecurity	com.app.applaunch20	4d9af2be2c55cf306391b10cc1c893f00205e5590c0f5b59e20e2d0b994cffdc
iSecurity	com.app.applaunch	70842ada0a36eb9448797c4168bd46ac6d523cfccf6e53f79f8e40f2d5c1a257

Copybara Samples

App name	Package name	SHA-256
BNL Token	com.apk.bnl.token	30b40d95bdd149ba5636de91b80aa60421d1d148032d65f9a8d4f36ef0e0de55
Banca Sicura	com.com.gruppoisp.app	7cc62bd300b83dab0d12045bb8a0f82bf80ac4c8885922f7156f1766b4cc5c7a