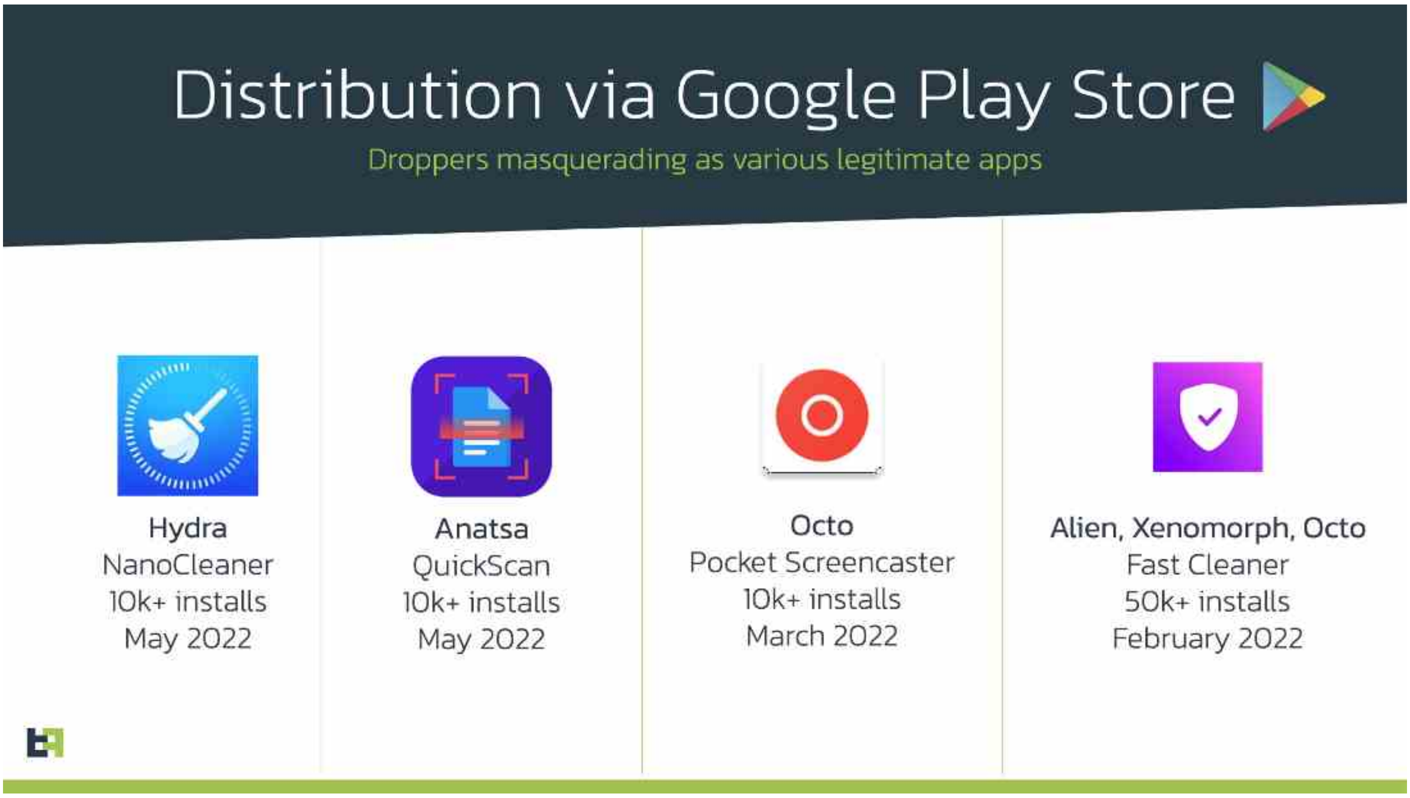
2022 mobile threat landscape update

May 2022

Intro

2022 started with several new Android banking Trojans appearing on the threat landscape. At the same time, the existing ones are constantly updating their capabilities following each other's pace and introducing game-changing features. Our threat intelligence shows that malware families with ability to perform On-Device Fraud (ODF) are seen more and more often, making it a worrying trend. To give a more tangible sense of the danger that these malware families pose, in this blog we showcase a demo of a Automated Transfer System (ATS) attack, which can be used to perform ODF.

In addition to this, ThreatFabric analysts continue to discover more droppers on Google Play having thousands of installations and distributing banking Trojans since the beginning of 2022.

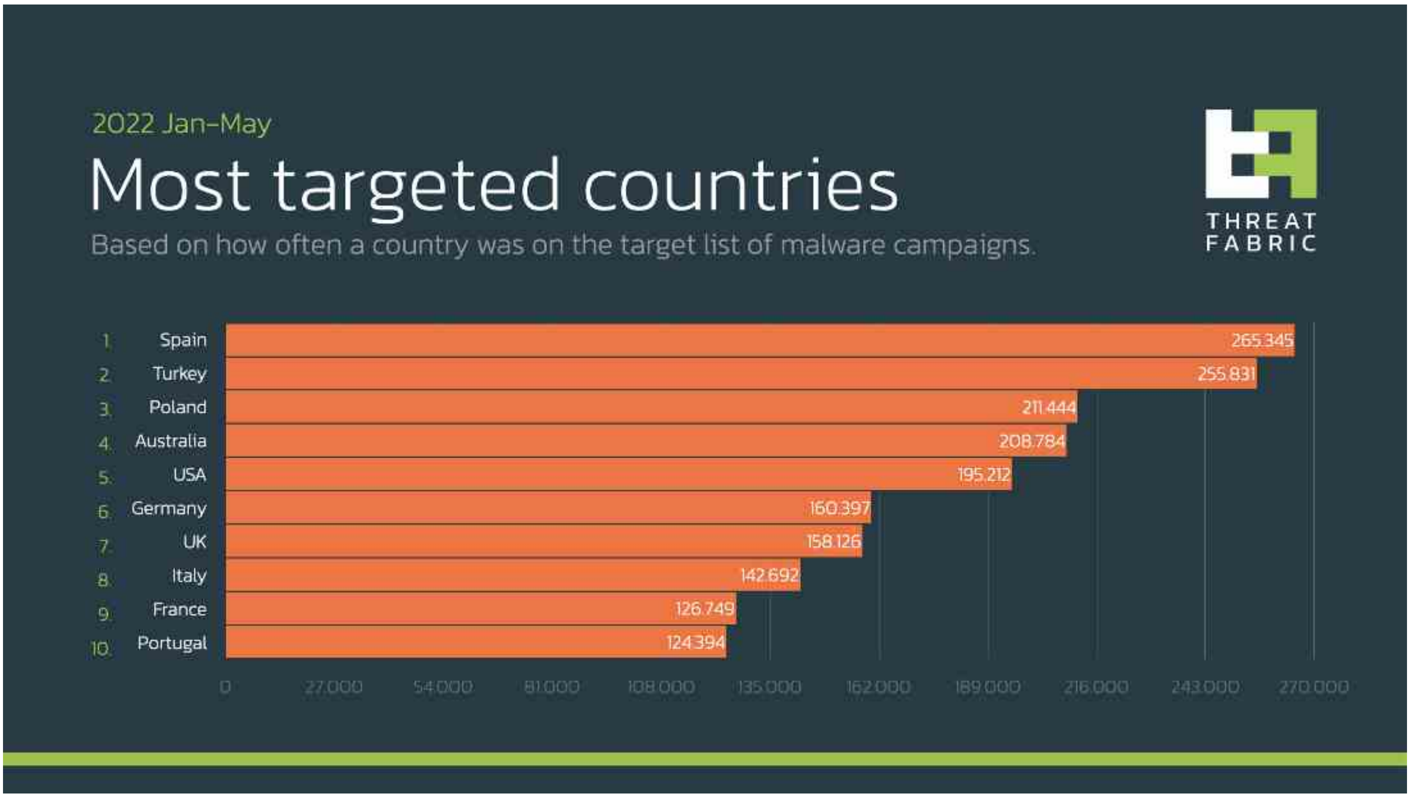


Finally, we will present a brief overview on how Google has introduced several updates in Android 13 that are designed to protect users against malware misusing Accessibility Service. However, our research team has successfully overcome these limitations and managed to avoid the new restrictions added in the new OS version.

This blog summarizes the current state of mobile threat landscape and gives insights on its possible future regarding the changing environment.

Threat landscape: focus on crypto and reliability

The start of the year brought several significant campaigns and a couple of new features introduced by different malware families. Our threat intelligence shows that Spain and Turkey are now the most targeted countries. Being compared to the same period in last year, Turkey is “catching up” with Spain, reducing the gap.

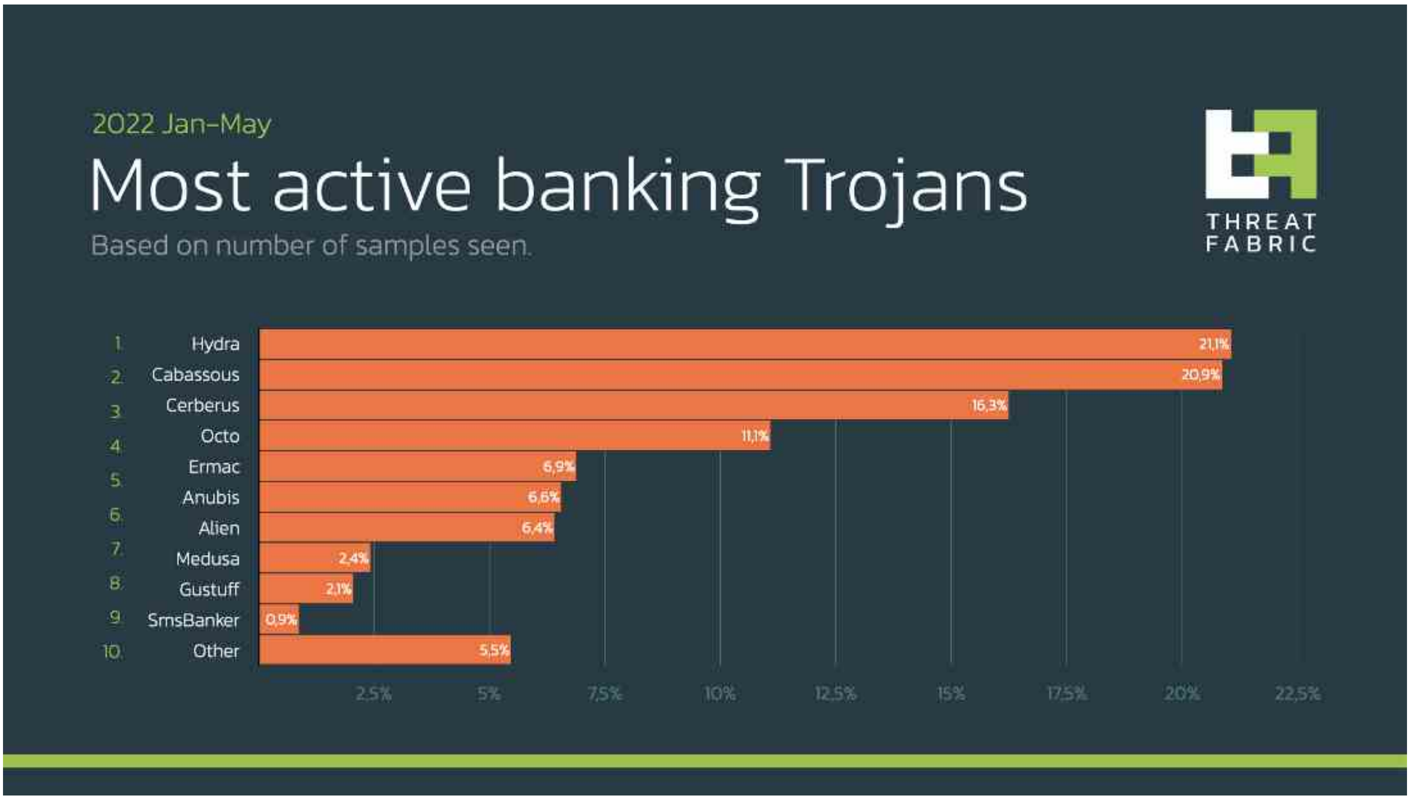


2022 Jan-May

Most targeted countries

Based on how often a country was on the target list of malware campaigns.

this trend is fueled by the raising activity of Turkish actors who are known to target their region with malware families like Hydra, Alien, and Cerberus. Such activity also "helped" these malware families take places in the Top-10 of the most active mobile banking Trojans in the beginning of 2022.



2022 Jan-May

Most active banking Trojans

Based on number of samples seen.

Octo: no one escapes the tentacles!

In our previous blog we uncovered that Octo botnet, actively promoted on darknet forums, is in fact a ExobotCompact inheritor and it is rented out to multiple threat actors. The main actor behind Octo keeps updating the Trojan and has introduced several new features in the latest update.

One of such features introduced in late April 2022 seems to be quite unique. In the new version the author of Octo has re-designed the overlays mechanism, so the Trojan is able to steal the credentials entered in overlay even if the form is not submitted. This is done in order to be able to get the credentials even if victim suspected something and closed the overlay without actually pressing the fake "login" present in the overlay page.

To achieve it the Trojan overwrites the overlay's HTML code adding the "onblur" event to the code. This event happens every time when the UI object loses focus, thus Octo tries to capture the moment when user entered data and switched to another field.

Moreover, given that Octo overwrites the overlay within the bot code, actors are able to use "third-party" overlays provided by other actors as a service and do not have to change them on their own. The following code snippet shows the explained process:

```
this.fieldNames = new String[]{"email", "month", "number",
                                "password", "search", "tel",
                                "text", "time", "url", "week"};
...
private String prepareOverlay(String target, String overlayData, String overlay
    if(overlayType.equals("url")) {
        return overlayData;
    }

    String[] fieldNames = this.fieldNames;
    int index;
    for(index = 0; index < fieldNames.length; ++index) {
        overlayData = overlayData.replace(
            "type=\"" + fieldNames[index] + "\" ",
            "type=\"" + fieldNames[index] + "\" onblur=\"Android.on_blur_send(t
    }
...
}
```

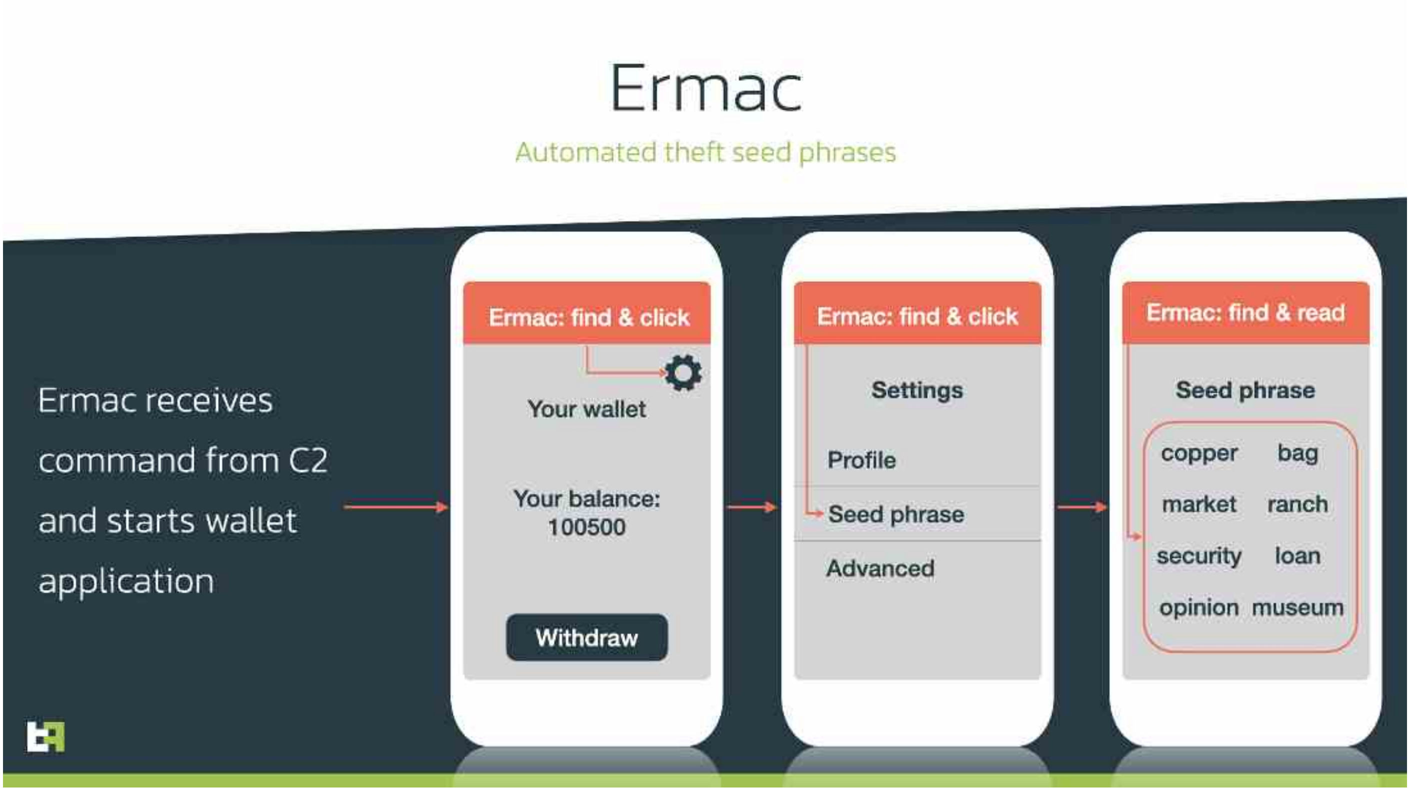
This update definitely helps actors to obtain even more data from victims and ensures reliability of the stealing process. Being powered with VNC and capable to perform On-Device Fraud (ODF), Octo remains one of the most dangerous Trojans on the current mobile threat landscape.

Ermac: theft automated

Another very active Trojan on the threat landscape is Ermac, which recently also received several updates. Compared to other malware families, Ermac really stands out in its focus on cryptocurrency related targets. Recently, these efforts resulted in the addition of specific code to perform automated stealing of seed phrases from different cryptocurrency wallets.

A seed phrase is a random set of words that can be used in order to restore access to the wallet. Once stolen, it can be used by cybercriminals to obtain access to the wallet and perform transactions there. Such phrases are stored inside crypto wallet apps in case users need access to them.

This fact led Ermac authors to introducing a feature that can steal seed phrases from multiple wallets. To do so, authors abuse AccessibilityService to perform actions and read the contents of the screen. Ermac has a built-in Accessibility engine that supports several wallets and contains specific set of actions to perform for every targeted wallet. Since the seed phrase is located on one of the pages inside the app, Ermac performs several actions to reach this page and read the content of it. The process of such automated theft is described on the picture below:



Ermac

Automated theft seed phrases

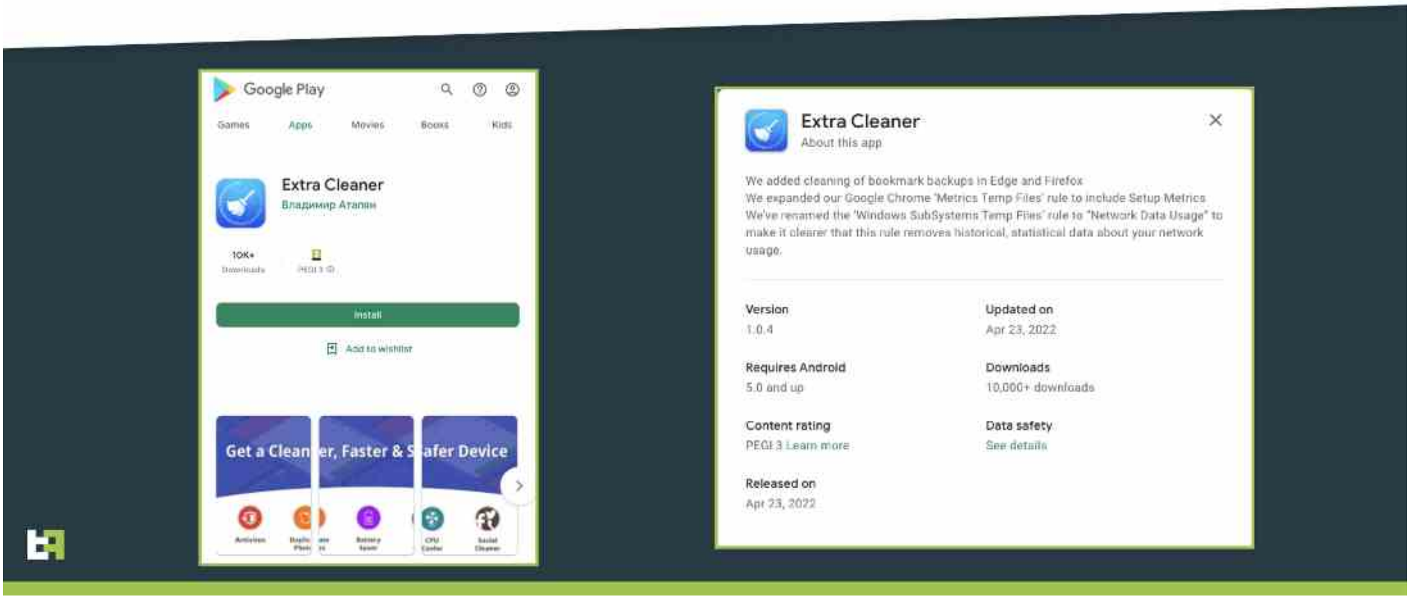
Ermac receives command from C2 and starts wallet application

The concept is not new as other malware families use the same approach to perform actions on victims' behalf which result in On-Device Fraud (ODF). The same goes for Ermac – while we have not seen it performing ODF, such semi-automated attacks are a worrying trend on the current threat landscape, and we expect more malware families absorbing this approach.

Google Play distribution

Dropper on Google Play

10k+ installations



Extra Cleaner
Владимир Атапин
10K+
Downloads

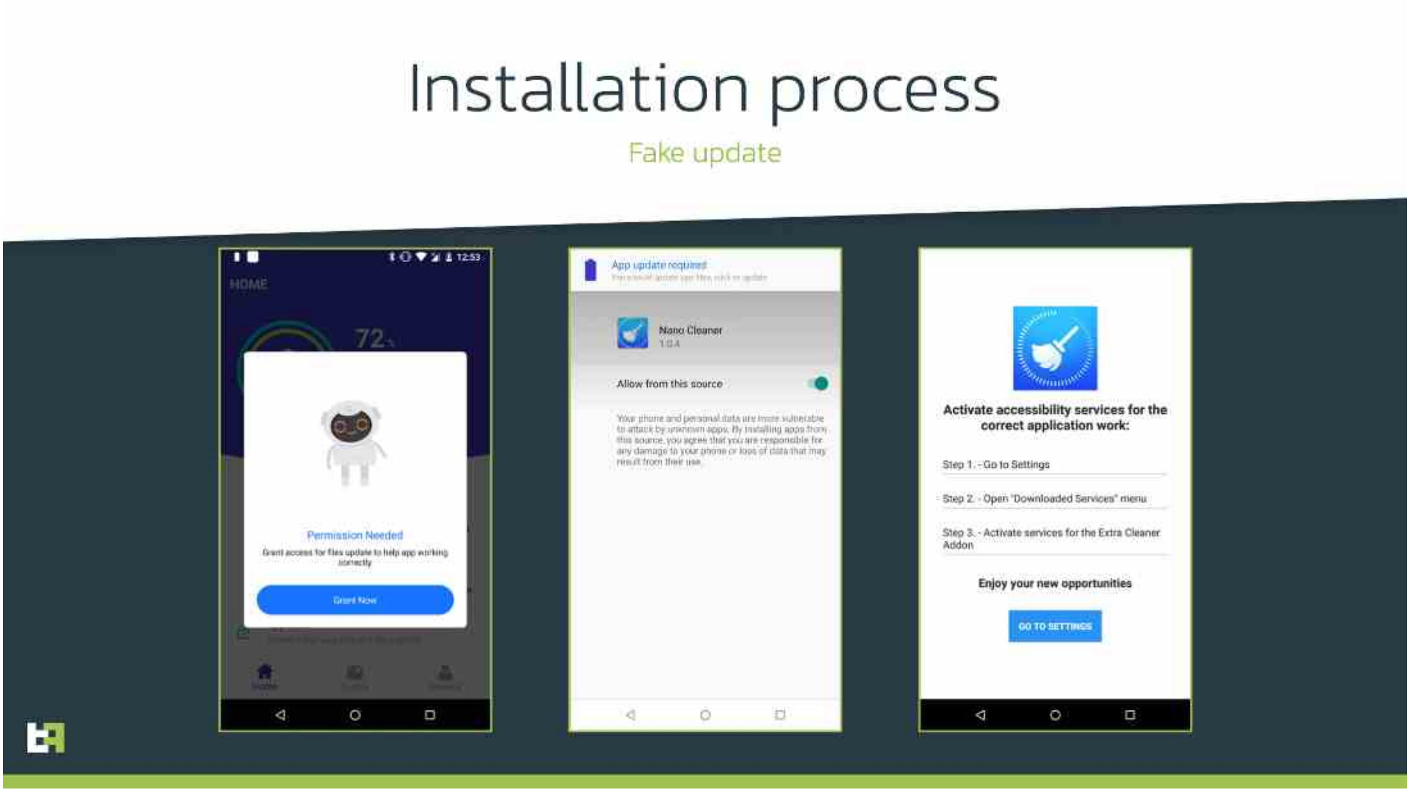
Extra Cleaner
About this app

We added cleaning of bookmark backups in Edge and Firefox
We expanded our Google Chrome 'Metrics Temp Files' rule to include Setup Metrics
We've renamed the 'Windows SubSystems Temp Files' rule to "Network Data Usage" to make it clearer that this rule removes historical, statistical data about your network usage.

Version 1.0.4	Updated on Apr 23, 2022
Requires Android 5.0 and up	Downloads 10,000+ downloads
Content rating PEGI 3 Learn more	Data safety See details
Released on Apr 23, 2022	

Threat actors continue to consider droppers on Google Play as one of the most effective ways to deliver malware to victims: being installed from the official store, an app is less likely to be doubted when asking for some suspicious actions.

One of the latest droppers discovered by ThreatFabric is posing as cleaner app and has 5k+ installations. It operates similarly to other known droppers, downloading the payload from GitHub and installing it. During this campaign ThreatFabric analysts observed this dropper distributing Hydra, a mobile banking Trojan that is also on the rise in terms of number of samples seen in-the-wild. Hydra is a well-known Trojan armed with RAT capabilities; thus it is also able to perform On-Device Fraud (ODF). The following screenshots show the process of payload installation:



Installation process

Fake update

Permission Needed

Grant access for files update to help app working correctly

App update required

Nano Cleaner
1.0.4

Allow from this source

Your phone and personal data are more vulnerable to attack by unknown apps. By installing apps from this source, you agree that you are responsible for any damage to your phone or loss of data that may result from their use.

Activate accessibility services for the correct application work:

Step 1. - Go to Settings

Step 2. - Open "Downloaded Services" menu

Step 3. - Activate services for the Extra Cleaner Addon

Enjoy your new opportunities

Just like most of mobile banking Trojans, Hydra first requests enabling AccessibilityService in order to present overlays and perform actions on the infected device.

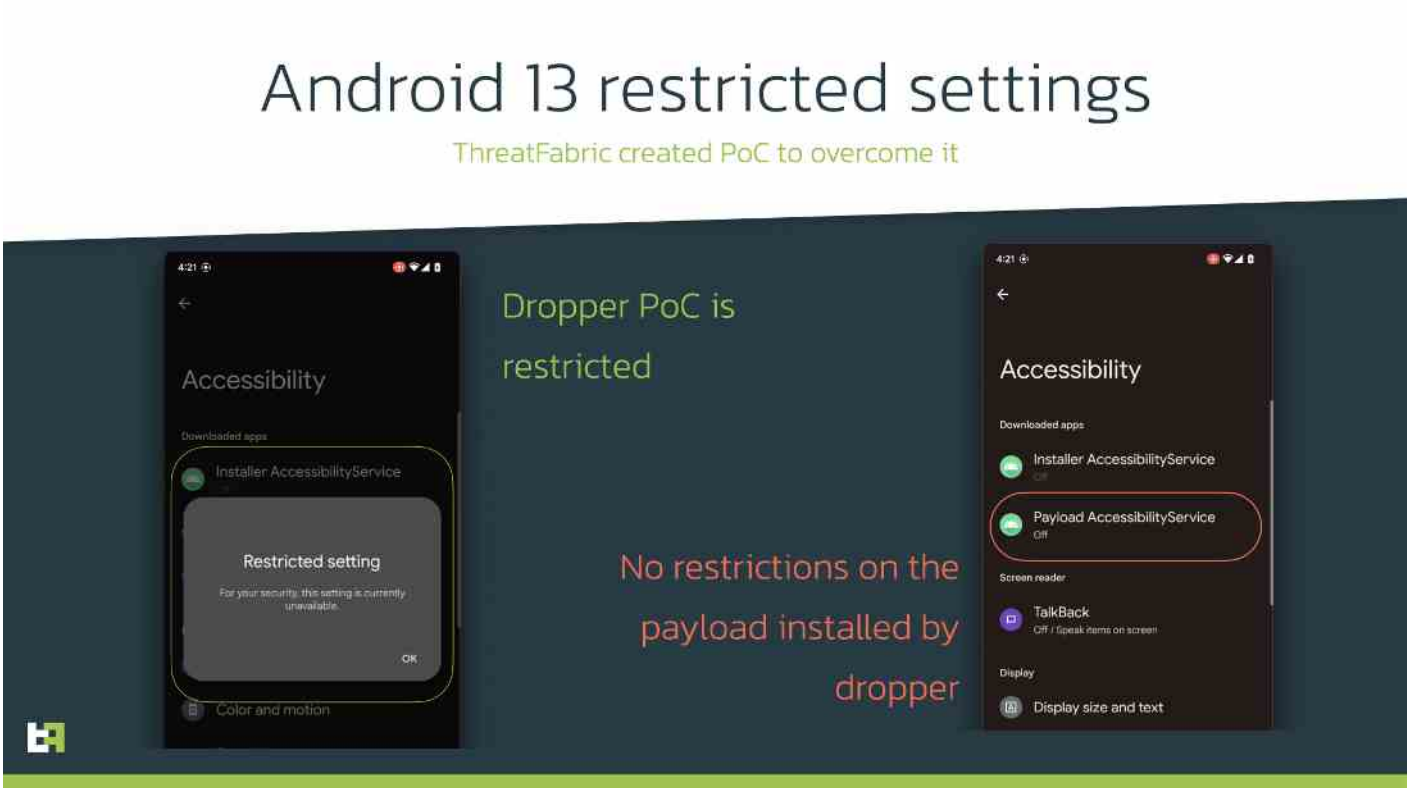
Android 13 Restrictions

Google decided to finally address the issues generated by the Abuse of Accessibility Services.

The beta version of Android 13 presents a new approach to enabling AccessibilityService of applications installed from third-party sources. This new version features a new option called “restricted settings”, which include AccessibilityService.

In the case of a dropper installing a payload, user will not be able to easily enable AccessibilityService for it, as it will greyed out and unavailable by default. To enable it, user will have to perform more explicit actions and confirm it with device password.

However, our research shows that such mitigation is not enough and these restrictions can be fairly easily overcome. The following screenshot shows two proof-of-concept applications, one behaving like the droppers we usually encounter on Google Play Store, while the second uses a different technique with a slight change in installation process. Doing so, ThreatFabric researchers managed to avoid the restricted settings in the second PoC application.



Android 13 restricted settings

ThreatFabric created PoC to overcome it

Dropper PoC is restricted

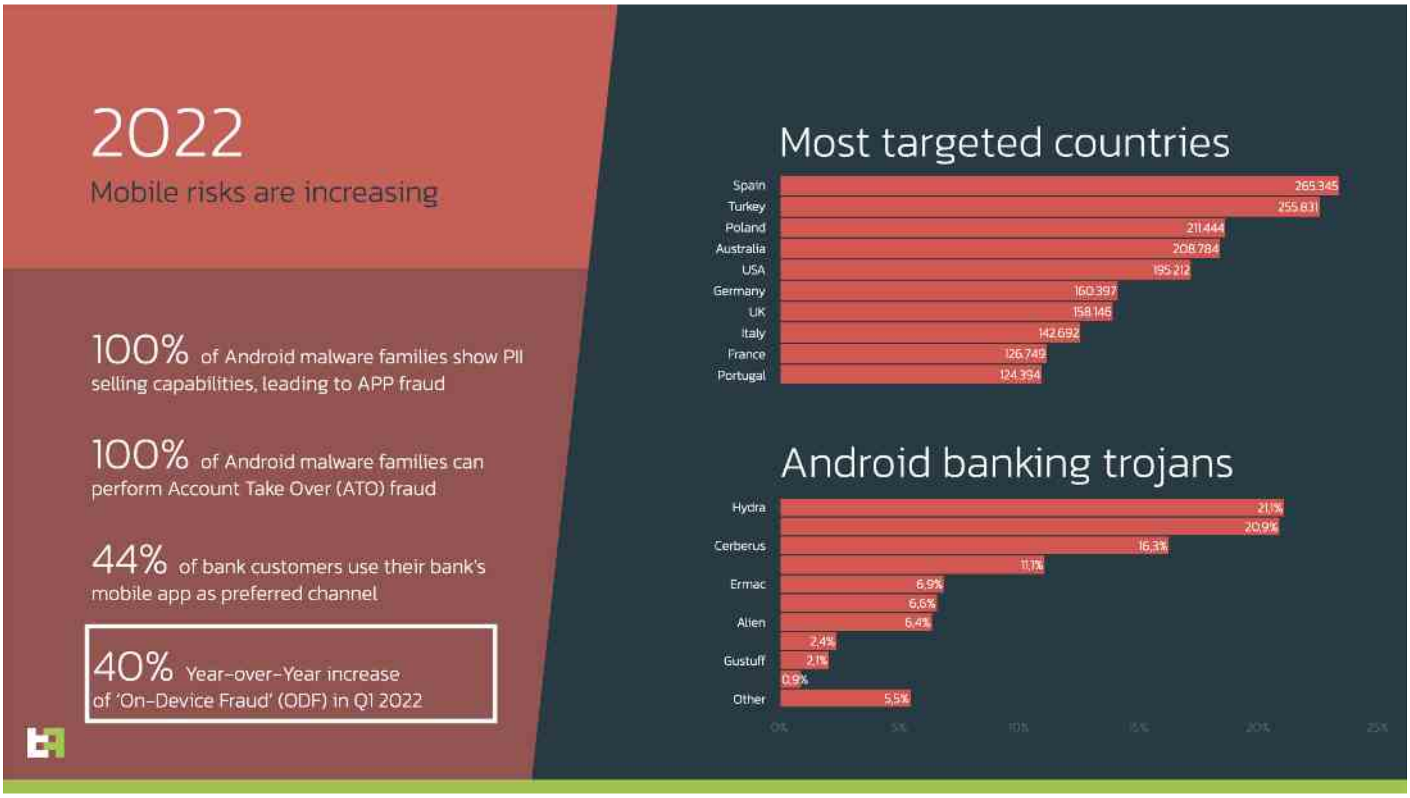
No restrictions on the payload installed by dropper

4:21
Accessibility
Downloaded apps
Installer AccessibilityService
Restricted setting
For your security, this setting is currently unavailable.
OK
Color and motion
4:21
Accessibility
Downloaded apps
Installer AccessibilityService
Off
Payload AccessibilityService
Off
Screen reader
TalkBack
Off / Speak items on screen
Display
Display size and text

Although introduced changes can protect users from certain malware on new version of Android, we believe that most of the actors will quickly adapt to the restrictions with a slight change in their MO until a stricter approach will be introduced. However, Android operating system is known for its openness and availability, so it is definitely a question of balance for developers. That is why it is necessary for financial organizations to pay more attention to the current landscape and oversee the changes of it.

On-Device Fraud

As it is clearly demonstrated by the section above, 2022 has been an extremely active year for Android Banking malware. This trend has been consistent and a continuation of what we have seen in 2021. As previously discussed, we have observed not only the appearance of new families in the Android threat landscape, but also the continuous improvement of existing ones.



2022

Mobile risks are increasing

100% of Android malware families show PII selling capabilities, leading to APP fraud

100% of Android malware families can perform Account Take Over (ATO) fraud

44% of bank customers use their bank's mobile app as preferred channel

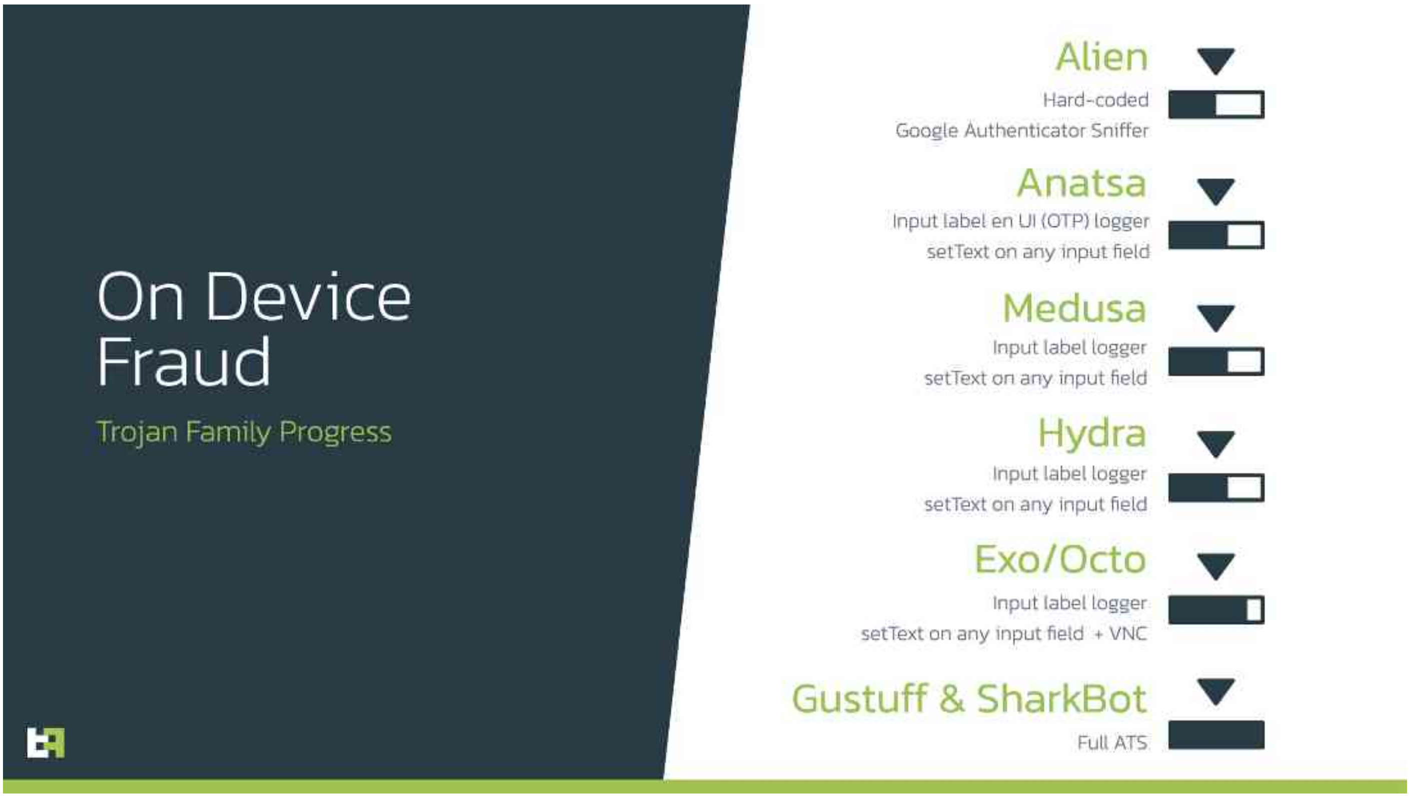
40% Year-over-Year increase of 'On-Device Fraud' (ODF) in Q1 2022

From ATO to ODF

We are witnessing an Android banking malware spring season, where the full focus and attention by criminals is changing and switching very rapidly from the Account TakeOver (ATO) modus operandi, to something more complicated, but also more lucrative: in fact, more and more malware families are now implementing some sort of On-Device Fraud (ODF) capability.

Every banking family that we observe currently presents ATO capabilities.
If ATO malware, which relies on credential theft to be used on a separate channel, was predominant a few years back, nowadays ODF seems to be the new requirement for new Android banking malware. Based on our Threat Intelligence, ThreatFabric has observed a 40% increase or ODF malware in Q1 of 2022.

Most families that are currently active implement some degree of ODF, ranging from the ability of modifying UI fields like username and password text boxes, to the capability of logging in a banking application and transfering funds automatically by downloading and executing fully programmable scripts (ATS - Automated Transfer System).


On Device Fraud
Trojan Family Progress
Alien
Hard-coded
Google Authenticator Sniffer
Anatsa
Input label en UI (OTP) logger
setText on any input field
Medusa
Input label logger
setText on any input field
Hydra
Input label logger
setText on any input field
Exo/Octo
Input label logger
setText on any input field + VNC
Gustuff & SharkBot
Full ATS

In the case of malware families like Gustuff and Sharkbot, which implement full ATS, criminals are able to define a specific set of actions, based on Android version, device manufacturer, and banking application, to be executed to achieve their goals. These action include, but are not limited to, enabling installation from unknown sources, granting themselves permissions, using stolen credentials to login in the banking application, checking balances and performing transactions.

All the above actions happen on the victim's device, and unless some behavioural analysis is performed, a transaction completed with this attack MO will look no different from a legitimate one from the point of view of a fraud scoring engine.

ATS Demo

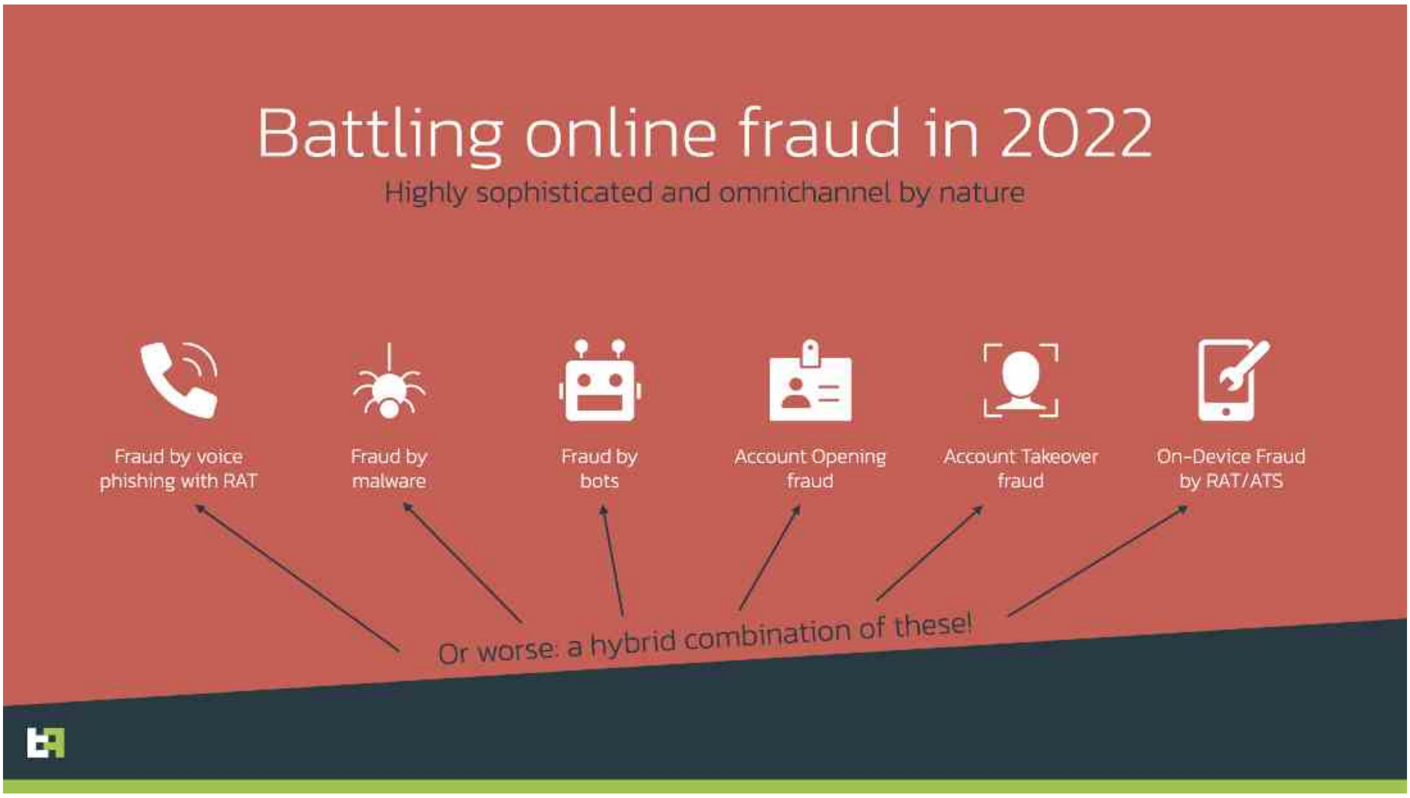
To give a better understanding of what ODF looks like, we developed a Proof of Concept (PoC) ATS malware, designed to attack a fictitious banking application. In the following video you will see how malware can interact with the UI and successfully login using previously stolen credentials and perform a transaction. The steps are slowed down to allow the viewer to understand what is happening. However, in a real case scenario, the whole process would happen in a few instants, leaving no time to react to the victim.

With capabilities like ATS and other Accessibility Service powered features, it is clear that even if a malware variant is not targeting a bank with overlays, it can still perform a large variety of attacks. For this reason it is vital to have preventive and pro-active detection solutions in order to prevent this attacks before they are initiated.

How to deal with possible infections and fraud

What to do in the unfortunate event of a fraud attempt?

If an financial institution or a customer suspects being victim of some sort of fraud, a contact with the technical assistance team is the first step in understanding what happened and helping the potential victim.



Battling online fraud in 2022
Highly sophisticated and omnichannel by nature
Fraud by voice phishing with RAT
Fraud by malware
Fraud by bots
Account Opening fraud
Account Takeover fraud
On-Device Fraud by RAT/ATS
Or worse: a hybrid combination of these!

What follows is a list of questions to ask potential victims, whose answers could help in assessing the likelyhood of actual fraud, combined with suspicious transfers observed from the banking institution side and other fraud indicators:

- **Do you remember if you have recently installed any new application? Was that application installed from Google Play store or from a third-party source?**

The first step in any infection chain is the installation of a new application, may that application be a dropper or the malware itself. In addition, applications installed from sources other than Google Play Store, like third-party markets or websites, are more likely to be dangerous. As previously discussed, installing from Google Play Store is not fully safe either, but it is still preferable to the alternative.

- **Have you given some unusual permission or enabled something (like for example Accessibility Services)?**

Most modern Android malware is able to grant itself all the permissions required to execute its nefarious code. However, in order to do so, the user will have to manually grant one single privilege to the malware. That is the Accessibility Services privilige. Without this, the malware is not able to interact with the UI and simulate button clicks and text inputs.

- **Was your device acting strangely? Examples of this might be: flashing screens, blinking windows, login asked for the first time in a while.**

When malware executes, it will grant itself a series of permissions needed to interact with the system, like the permission to manage SMS, Notifications, Camera, and so on. To do so, it will generate a pop up on the screen and then automatically click it thanks to Accessibility Services. To the user, this behaviour will look like a series of screens popping up and disappearing instantly.

- **Were you contacted by your bank?**

Criminals also often impersonate technical assistance personnel of the bank to convince users to install malware on their device. In these cases, the operator will ask to install some application that could be either malware or Remote Access Software that will grant criminals full access to the device.

Manipulating the customer journey

Customer devices as the frontline of modern fraud

BANK
Create & secure banking apps
Infect customer devices & manipulate banking apps
"Hi, this is your bank speaking!"

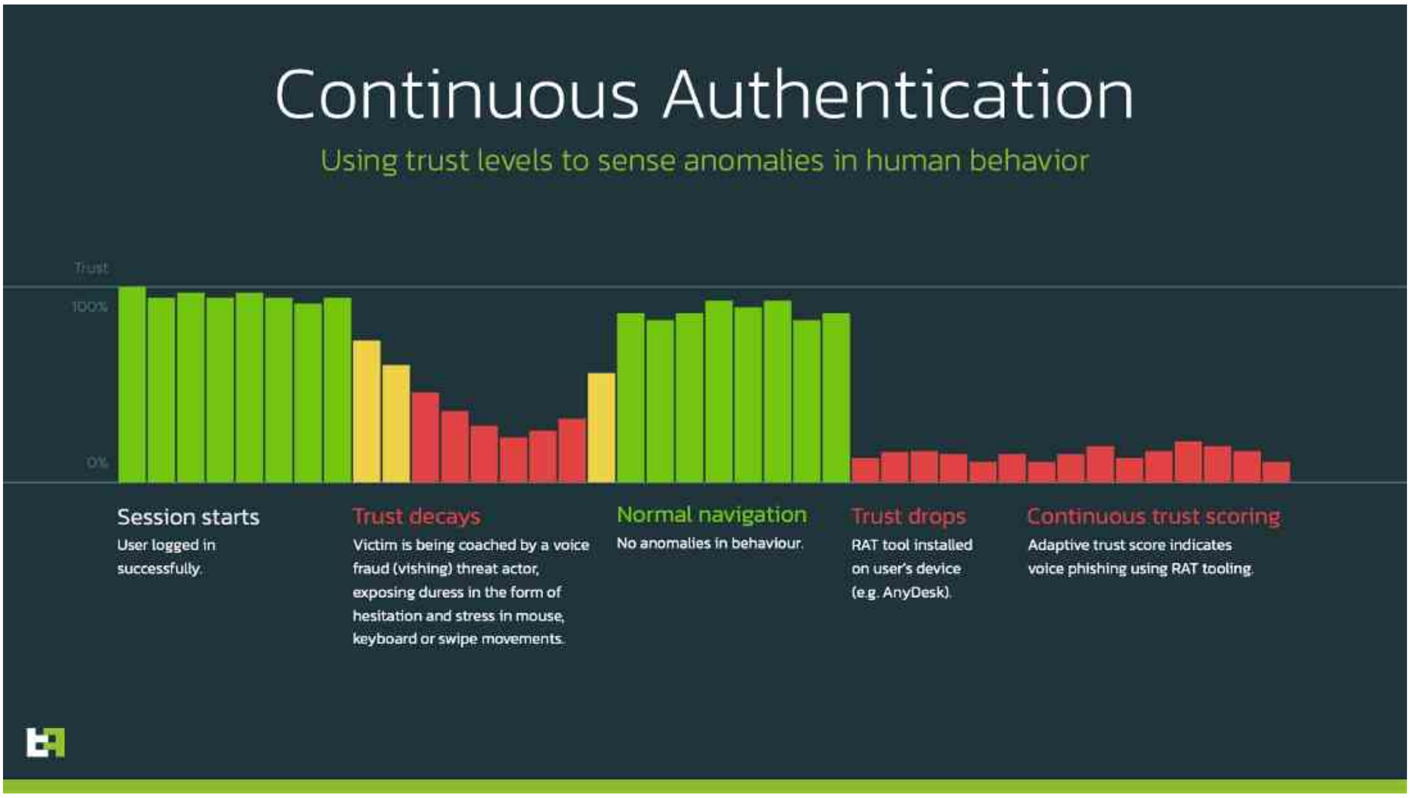
In case of confirmed infection, what should a customer do?

Unfortunately, there is no silver bullet in case of infection. Different malware operates differently, and for the average user, uninstalling the malware can be very hard if not impossible. In this cases, the only process that we can recommend is a full factory reset of the device together with a change of all credentials, both for banking applications as well as social media apps and cryptowallets.

How to mitigate risks?

With the growing number of active malware families that can perform On-Device Fraud, it has become a challenge for fraud prevention/detection departments to prevent and investigate fraud coming from the same device that customer uses every day. To understand the real impact and prevent losses a proper solution should be in place to gain visibility on the malware infecting customers' devices. Moreover, solution should provide visibility not only on the known malware or already seen samples of it (so-called hash-based detection) but to detect unknown malware relying on its malicious behaviour. Such approach allows to have full picture of possible risks that can be properly mitigated.

Proper on-device detection of malware also helps to gain visibility on distribution channels and proactively notify customers about new distribution campaigns to raise their awareness. Powered with continuous authentication based on behavioural biometrics, such solution becomes a great source of TI-based risk-score for every account and makes fraud detection and prevention easier for financial organisations.



Continuous Authentication

Using trust levels to sense anomalies in human behavior

Session starts

User logged in successfully.

Trust decays

Victim is being coached by a voice fraud (vishing) threat actor, exposing duress in the form of hesitation and stress in mouse, keyboard or swipe movements.

Normal navigation

No anomalies in behaviour.

Trust drops

RAT tool installed on user's device (e.g. AnyDesk).

Continuous trust scoring

Adaptive trust score indicates voice phishing using RAT tooling.

Conclusions

The start of the year gives no surprise in the mobile threat landscape. The On-Device Fraud (ODF) trend we predicted in 2021 continues and we expect more and more malware families to implement ODF capabilities. The openness of Android OS serves both good and bad as malware continues to abuse the legitimate features, whilst upcoming restrictions seem to hardly interfere with the malicious intentions of such apps, as we proved in our PoC.

Anti-fraud departments in financial organisations are now facing the ever-growing problem of On-Device Fraud and should have proper mechanisms providing them with visibility on the threat landscape and existing risks within their customers. This is only possible with TI-based on-device malware detection in place, allowing to foresee the changes of the threat landscape.

MTI & CSD

Our Mobile Threat Intelligence (MTI) service provides financial institutions with a better visibility on the increasing threat of mobile banking malware. Banks who are using MTI understand which malware campaigns are targeting their mobile channel and how their mobile banking users are impacted.

With our Client Side Detection (CSD) service we are helping financial institutions to gain visibility on (potential) fraud by mobile banking malware, and to prevent it. If you would like to know more about how we use our mobile threat intelligence to detect mobile banking malware on mobile devices, feel free to reach out to sales@threatfabric.com.

Appendix

Droppers on Google Play

App name	Package name	SHA256 Hash
Nano Cleaner	com.casualplay.leadbro	d5ac8e081298e3b14b41f2134dae68535bcf740841e75f9
QuickScan	com.zynksoftware.docuscanapp	e05dac61b4b27e90d3f4c832a76fa52e9065e894b8b8c

Octo Samples

App name	Package name	SHA256 Hash
Chrome	com.talkleadihr	1ad466c63462ac0e7579bdf6201a6a527af8112c5d7ac857da19064
Play Store	com.girltold85	0c4b6bc01923b5937627485d816de856d864cf0cc83623066d4b9
Pocket Screencaster	com.cutthousandjs	01edc46fab5a847895365fb4a61507e6ca955e97f5285194b5ec60e

Ermac Samples

App name	Package name	SHA256 Hash
Chrome	com.biyitunixiko.populolo	26fa10489a189fab2a255d8f54d841d2316ce8e4f7d49fc3963349
Chrome Mobile	com.xifoforezuma.kebo	f18fb17d6131493eb2f407706a11942b4846fe67d686836c6ba6b2
BAWAG PSK Security	com.qjlpfydjb.bpycogkzm	0ec3aba023da64c28c3e664ba83a337782c855f3b39874cde59f