

# The State of Android (Banking) Malware

Insights from 2022 and Predictions for 2023

T L P : W H I T E



ThreatFabric BV

Naritaweg 132

1043 CA Amsterdam

E-mail: [info@threatfabric.com](mailto:info@threatfabric.com)

Web: [www.threatfabric.com](http://www.threatfabric.com)

This document was written by ThreatFabric BV. The information in this document may not be modified or copied without prior consent of ThreatFabric BV

ThreatFabric and its logos are trademarks of ThreatFabric BV. The trademarks, names and illustrations of other organizations and products are the property of the relevant owner.

The information in this document, including possible attachment(s), is confidential and intended exclusively for the addressee. Publication, reproduction, distribution or consultation of this document is permitted only with explicit permission of ThreatFabric BV or the addressee.

© ThreatFabric BV, All rights reserved.



## Reviews

Date	Version	Description
February 22, 2023	v1	Initial Report



## About this Document

This document is meant for the creation of an overview of trends seen or observed by ThreatFabric researchers for the year 2022 and its relevant predictions for 2023. It is entitled for ThreatFabric prospects, customers and registered partners, the content of the document is meant for use of such parties only.

# Table of Contents

<b>1. Year in numbers .....</b>	<b>4</b>
1.1 Volume Analysis .....	4
1.2 Geographical Targets.....	5
<b>2. Most active and notable malware families .....</b>	<b>7</b>
2.1 Ermac.....	7
2.2 Octo.....	8
2.3 Hydra.....	8
2.4 SharkBot.....	10
<b>3. Spyware and RAT: A Constant Threat.....</b>	<b>13</b>
3.1 Spyware .....	13
3.1 Remote Access Tools and ATS.....	15
<b>4. Trends and predictions .....</b>	<b>23</b>
4.1 Phishing Attacks Targeting Financial Sector in 2022 .....	23
4.2 Droppers in Google Play .....	25
4.3 Everything-as-a-Service (XaaS).....	28
4.4 Increasing the target surface .....	31
<b>5. Conclusions.....</b>	<b>34</b>

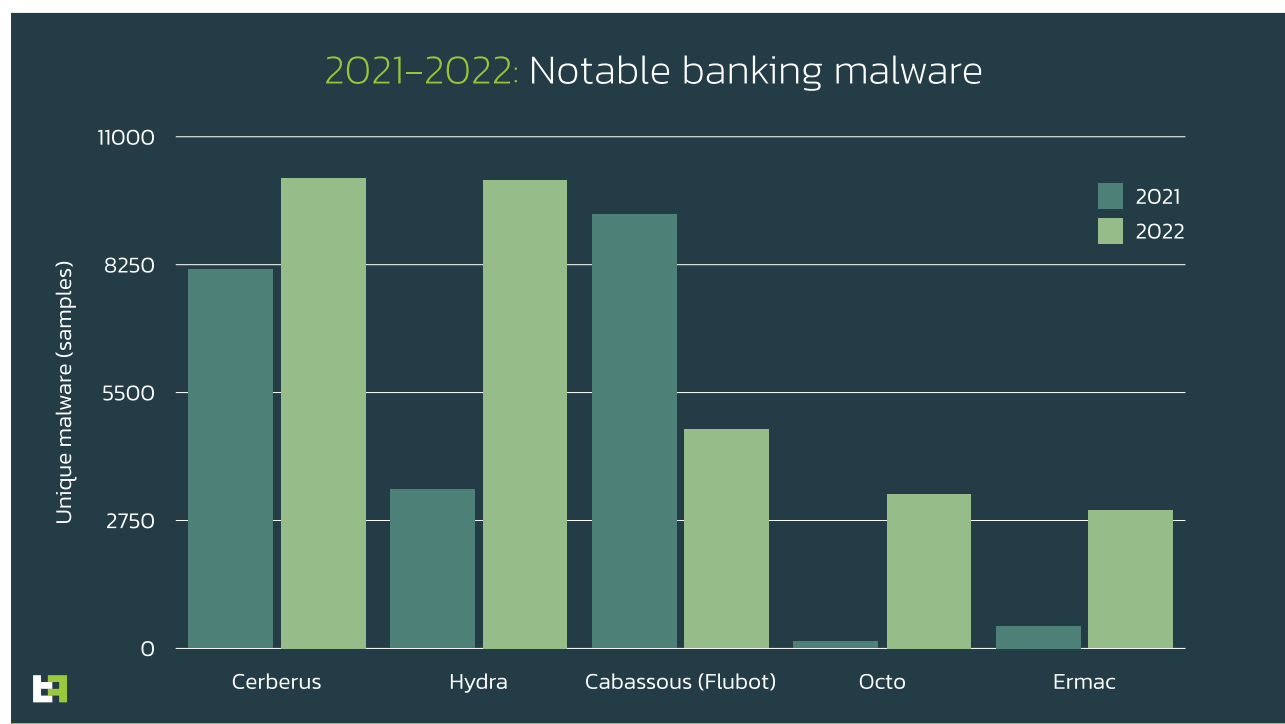
# 1. Year in numbers

The incredibly growing popularity of rental malware families, the appearance of new names on the landscape, **twice as many more malicious droppers** on official application stores: these are a few of the trends that ThreatFabric identified this year – in this section we provide a review of the numbers in 2022 based on our threat intelligence.

## 1.1 Volume Analysis

2022 has brought many new names on the mobile threat landscape, as well the updates to the already known malware families. ThreatFabric has identified **30+** new variants of financially oriented banking malware, indicating a continuous evolution taking place on the mobile threat landscape.

At the same time, several malware families gained more “popularity” in 2022. As an example, **Hydra**, banking Trojan with RAT capabilities, was detected almost **3 times more often** compared to 2021.



*Most notable (in numbers) banking malware families in 2021-2022*

Another example is **Ermac**, which gained popularity amongst cybercriminals after its first appearance in July 2021. ThreatFabric analysts were able to identify multiple actors leveraging Ermac: its unique capabilities, like for example automated seed-phrases stealer for cryptocurrency wallets, are appreciated by multiple buyers on darknet forums. Moreover, the latest evolution of

Ermac, called **Hook**, added RAT capabilities at the end of 2022 and already gained a lot of attention from the cybercriminals.

In 2021 Cabassous (also known as **Flubot**) was one of the most active malware families based on the number of unique samples seen. Actors behind it maintained one of the largest smishing campaign in history, generating unique builds for every download of the malware to avoid detection. After its takedown in May 2022, the number dropped to 0.

Last year was also remarkable in the number of malicious droppers on the official store identified by ThreatFabric. Our analysts identified **an increase of 200%** in the number of campaigns involving a malicious dropper on Google Play Store. Our TI shows that these droppers were distributing malware families such as SharkBot, Octo, Hydra, Alien, Xenomorph – all having remote access capability. We will cover more in depth this trend in Section 4.2.

## 1.2 Geographical Targets

When analysing threats, ThreatFabric pays a lot of attention to the areas of interest of the attacks and campaigns. This past year showed that more and more actors tend to target the same areas.

The top 10 most targeted countries have remained consistent compared with last year. The podium is still made up by **Spain, Turkey, and Poland**, with Spain overtaking Turkey in number of attacks seen targeting countries.

Such an approach is followed by actors behind Hydra (Turkey, Spain, Germany, Austria), Gustuff (Australia), Octo (European countries).



*Most targeted countries in 2022 (MTI Portal data)*



In 2022 apps from Portugal were targeted more often than the year before, at the same time Russian-based applications were targeted less. The reason behind it might be the decreased activity of Anatsa and Anubis, whose target lists regularly included applications from Russia. Our analysts have also seen several efforts from Russian-speaking cybercriminals on darknet forums forbidding renting the malware that targets CIS countries.

The **geopolitical situation** does not leave actors neutral. However, usually it reflects not their political views, but the will to use the current situation to **maximize their financial gain**.

In mid-summer Anatsa, which is operated by Russian-speaking actors, was observed for the time targeting **Ukrainian banking applications**. ThreatFabric believes that this does not reflect the political views of the actors, as previously Anatsa consistently featured Russian banking applications as a part of its target list.

When we look at the threat landscape from the malware families' perspective, we see a clear change in top-10 most active malware families due to recent updates and newcomers. The following section highlights the most active and notable Android Banking Trojans in 2022.



## 2. Most active and notable malware families

### 2.1 Ermac

The malware family first appeared in July 2021, as the new project for Blackrock's author, **DukeEugene**. Supported by advertisements on darknet forums and constant updates adding new unique features, Ermac managed to gain popularity amongst the cybercriminals renting it.

The malware was recognized for its stability on the infected device and unique feature of stealing **seed-phrases** from cryptocurrency applications by other cybercriminals. This feature allowed Ermac to automatically click through the targeted wallet application to get to the screen where seed-phrase was stored. Having this phrase, actors could enrol new device and get full access to victim's crypto assets.

Our latest findings show that DukeEugene has unveiled to the public another banking Trojan of his making in the beginning of 2023: **Hook**. However, our systems spotted the first samples of Hook in mid-December 2022. The analysis revealed that this malware variant is an evolution of Ermac, enhanced with a powerful remote access engine, allowing to automate remote actions.

We believe Hook will become the main product in DukeEugene's portfolio, slowly replacing Ermac. However, several forks created on the basis of the sold source code of the first Ermac version might still be active and evolving separately.

## Hook Android Banking Trojan

Device Take Over (DTO) capabilities



*Hook.A capabilities*

## 2.2 Octo

In 2022 our systems observed a lot of activity from **Octo (ExobotCompact)** – another powerful banking Trojan with RAT capabilities. Being a descendant of Exobot's latest variants, ThreatFabric kept the name ExobotCompact; however, the actor behind it refers to it as Octo.

ExobotCompact history goes back to 2018, with some hiatuses along the way until the end of 2021, when a new evolution of it was presented. While observing only less than 200 samples of ExobotCompact in 2021, in 2022 our systems spotted more than 3300 malicious samples classified as ExobotCompact (Octo), and this trend continues in 2023.

2022 became a renaissance period for this old family, as it was updated and rebranded before returning to the market. Being a rental malware family, Octo has multiple actors behind, managing different campaigns. Some of the actors use Google Play droppers to deliver Octo to victims' devices: ThreatFabric found 5 malicious droppers on the official store masquerading as different tools and distributing Octo. Such activity highlights a continuous trend on Google Play droppers that we cover in further sections.



Fast Cleaner  
50k+ installations  
February 2022



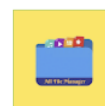
Pocket Screencaster  
10k+ installations  
March 2022



ScanGen  
10k+ installations  
August 2022



File Manager  
10k+ installations  
November 2022



File Manager – PDF Reader  
10k+ installations  
December 2022



*More than 100.000 reported installations from droppers on Google Play*

The malware uses built-in Android services, such as MediaProjection for screen streaming and AccessibilityService to perform actions remotely.

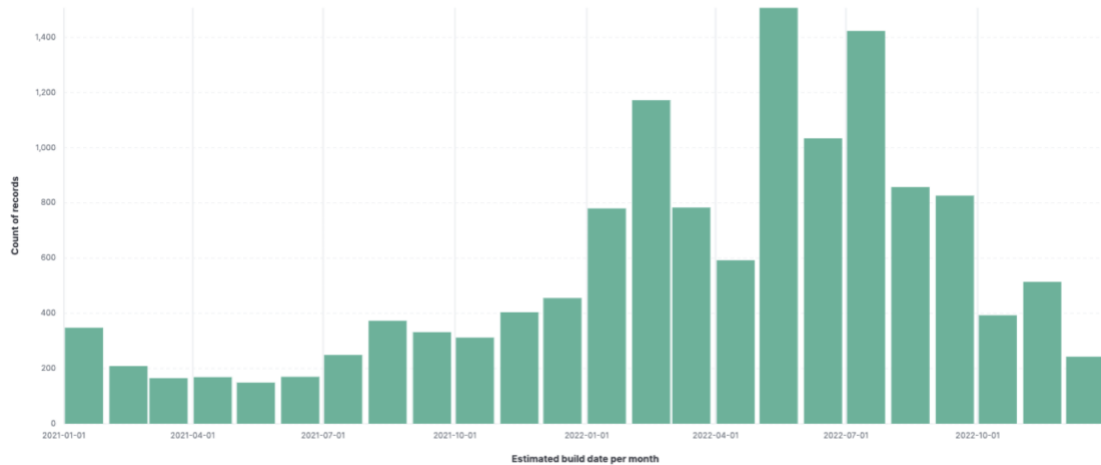
## 2.3 Hydra

In 2022 ThreatFabric analysts observed a significant increase in number of malicious samples classified as Hydra banking Trojan. The following graph represents the jump in numbers starting at

the beginning of 2022 with a peak in May 2022. It is worth noting that the peak coincided with the takedown operation of the network infrastructure of the Cabassous banking trojan.

## Hydra samples 2021 – 2022

MTI portal data



*Increase of samples of Hydra between 2021 and 2022*

Our analysts were able to identify at least **two separate groups** using forks of Hydra maintained (and rented) separately. One was mostly targeting **Turkey**, while the second was seen mostly used in **European and global campaigns**.

## Hydra campaigns

Targeting different regions, MTI Portal data

Malware variant	Malware types	C2s	Upload date / Build date
Hydra.C	RAT Banker	lanagarza441jol	22/01/2023 19:08 18 days ago 23/12/2022 16:08 a month ago
C2s Targets			
Hosts targets (30)			
App			
ŞEKER MOBİL ŞUBE (tr.com.sekerbilisim.mbank)			
Garanti BBVA Mobile (com.garanti.cepbesi)			
Gmail (com.google.android.gm)			
Enpara.com Cep Şubesi (finansbank.enpara)			
(samsung.settings.pin)			
Akbank (com.akbank.android.apps.akbank_direkt)			
Albaraka Mobile Banking (com.albarakaapp)			
İçcep - Mobile Banking (com.pozitron.icep)			
Turkcell Digital Operator (com.tech.android.onlineilem)			
ING Mobil (com.ingbanktr.ingmobil)			
Previous 1 2 3 Next			

Malware variant	Malware types	C2s	Upload date / Build date
Hydra.C	RAT Banker	9 C2s	26/12/2022 13:07 a month ago 25/12/2022 22:03 a month ago
C2s Targets			
Hosts targets (361)			
App			
Banco de Occidente Móvil (com.grupoavaloc1.banca...)			
Bancaperta (it.creval.bancaperta)			
Bankinter Móvil (com.bankinter.launcher)			
Santander Empresas (es.bancosantander.empresas)			
Crédit Coopératif (com.credit_coop.android.mobileba...)			
Correos (es.correos.widget)			
SambaMobile (com.samba.mb)			
Caf - Mon Compte (fr.cnaf.mobile.moncompte)			
YOOX - Fashion, Design and Art (com.yoox)			
Mobile Banking UniCredit (com.unicredit)			
Previous 1 18 19 20 37 Next			

Malware variant	Malware types	C2s	Upload date / Build date
Hydra.C	RAT Banker	1aewssas2s.com.de 1aewcfas22s.com.de 1aewcfas2s.com.de	24/01/2023 13:10 14 days ago 22/01/2023 10:19 16 days ago
C2s Targets			
Hosts targets (15)			
App			
ING Banking Austria (at.ing.diba.client.onlinebanking)			
(samsung.settings.pass)			
(samsung.settings.pin)			
Volksbank hausbanking (at.volksbank.volksbankmobile)			
Commerzbank photoTAN (com.commerzbank.photoTAN)			
BAWAG PSK klar - Mobile Banking App (com.bawagpsk.b...)			
Deutsche Bank Mobile (com.db.wccc.dbmobile)			
easybank App (com.easybank.easybank)			
Bank Austria MobileBanking (com.bankaustria.android.olb)			
SantanderSign (mobile.santander.de.smartsign)			
Previous 1 2 Next			

*Different Hydra campaigns: Turkey, Global, Germany and Austria*

In the beginning of 2023 Turkish law enforcement announced the **arrest of actors behind Hydra**. Based on our TI, we see that it was mostly likely only one of the actors behind Turkish “branch” of Hydra, while we still see **fresh builds targeting global market**.

ThreatFabric will keep monitoring the threat, while we expect that this arrest will not affect general activity of the malware family.

## Hydra Actor

Arrested in Turkey, still new samples globally

**News on actors' arrest**

Malware variant	Malware types	C2s	Upload date / Build date
Hydra.C	RAT Banker	hugomarcantumico.net topolacpolutunc.com paprangeruspasio.net rangetopolcunos.com	07/02/2023 01:42 11 hours ago 06/02/2023 22:07 14 hours ago
Hydra.C	RAT Banker	12 C2s	07/02/2023 01:43 11 hours ago 05/02/2023 19:15 2 days ago
Hydra.C	RAT Banker	ferdialacamelme.net	05/02/2023 13:09 2 days ago 04/02/2023 22:54 3 days ago
Hydra.C	RAT Banker	14 C2s	05/02/2023 01:27 2 days ago 04/02/2023 20:09 3 days ago
Hydra.C	RAT Banker	12 C2s	04/02/2023 23:25 3 days ago 04/02/2023 18:26 3 days ago

**MTI Portal with fresh samples**

Report of Hydra Takedown and recent Hydra samples

## 2.4 SharkBot

First spotted back in 2021, SharkBot underwent several update iterations over the past year. At the same time, most of its activity also happened during 2022, including distribution with Google Play droppers.

The most intriguing development introduced by the actors was related to **overcoming biometric authentication** in targeted applications and **automatic grabbing of sensitive data** from them.

To overcome biometrics authentication, the authors introduced a mechanism to automatically find and click “Cancel” button on the screen displaying the prompt to authenticate with fingerprint. This procedure, to which we refer as **Biometric downgrade attack**, allows actors to force the victim to log on their account with PIN code, which can be stolen with keylogging functionality of SharkBot.

This is also used to bypass the biometric authentication prompt when performing actual fraud on the infected device.



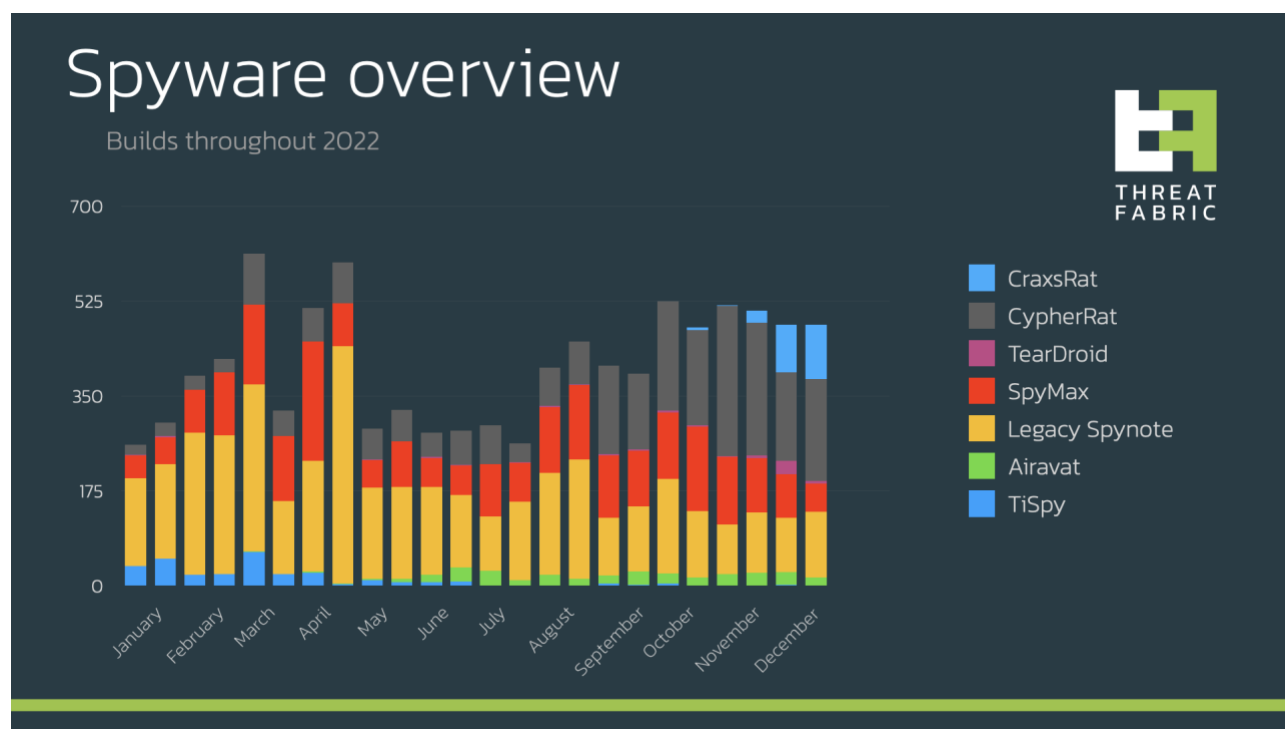


All the above techniques, combined with distribution through Google Play allowed actors to achieve high success rate in targeted regions (mostly UK and Italy) infecting unsuspecting customers.

## 3. Spyware and RAT: A Constant Threat

### 3.1 Spyware

The proliferation of Remote Access Trojans (RATs) and spyware in 2022 posed significant risks to individuals and organizations alike, presenting ongoing challenges for detection and prevention.

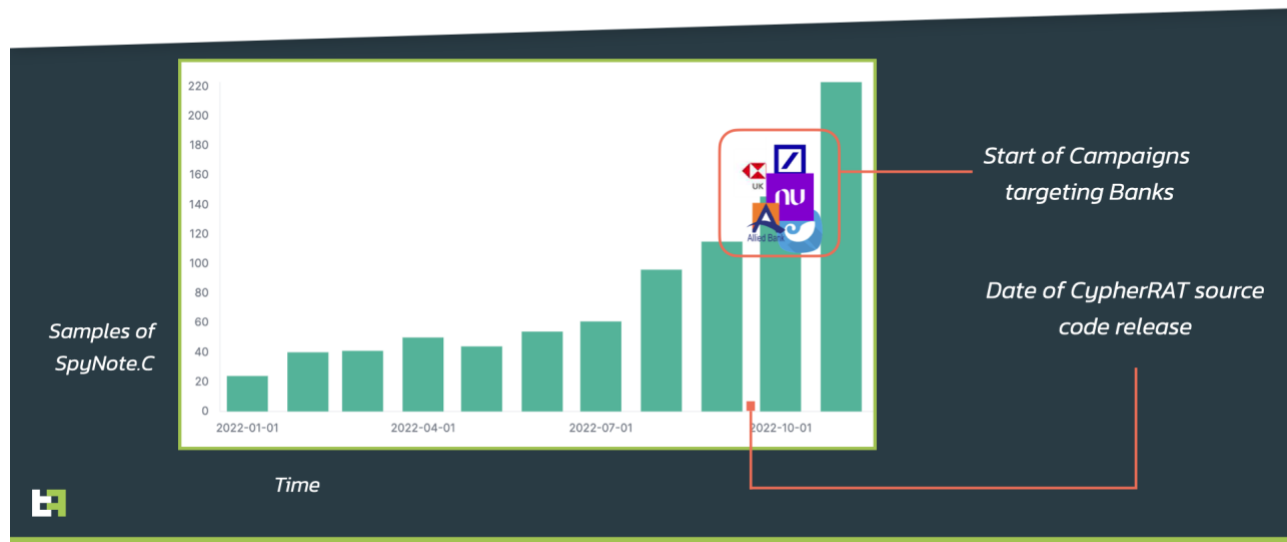


One of the most prominent examples of spyware is **CypherRAT**, also known as SpyNote.C by ThreatFabric. Its versatility enables attackers to tailor the malware to meet their requirements and specifically target victims, while its user-friendly interface makes it accessible even for novice hackers. SpyNote is primarily spread through phishing emails and social engineering, making it all the more challenging to guard against.

In the final quarter of 2022, ThreatFabric researchers noted a significant surge in SpyNote malware samples. The latest variant, SpyNote.C, is the most commonly used and accounts for the majority of spyware samples identified. Unlike its predecessors, SpyNote.C is actively targeting banking applications and impersonating **well-known financial institutions**, as well as popular apps such as WhatsApp, Facebook, and Google Play.

# SpyNote Targeting Banking

Substantial increase in volume



*SpyNote.C samples builds over the course of 2022*

However, in a recent development, the developer of CypherRAT has shifted their focus to a new spyware called **CraxsRAT**, which is tracked by ThreatFabric as **SpyNote.D**, demonstrating the constantly evolving nature of this threat.

## Craxs RAT (SpyNote.D)

New Project from Cypher Rat developer

*Craxs RAT website*

*Craxs RAT targeting banks*

Icon / App name / Package name	Malware family	Malware variant
Burlador Itau v3 (ate.initial.accurately) 3a57a6c3622b8a6f342187ad16b5d36fda8f96527001888eaa988d8d2de33ba4	SpyNote	SpyNote.D
BMG Novo (ts.dayton.transport) 9a6edff4dcaa9d0b8bae062617a2cb82f5ffdc1b5dc65befa1347dc75b0bfe9	SpyNote	SpyNote.D
Burlador Nubank v3 (tail.regression.hockey) c217b208d8dd82173dc661a94c2864fef0e1f1709742ae3b7ba5641bbf1e7eb7	SpyNote	SpyNote.D
Nifty and Bank Nifty (ins.il.capture) b08acef9886697876f592fff66d63284dd5f841e7b2342e9c68c45a6e768f069	SpyNote	SpyNote.D
targobank3 (capitol.skirts.thousand) 6282d778f67a8e5a95bead7a36ed7dc834b02825d7ab7be5b4a7ab499b4f4488	SpyNote	SpyNote.D

*SpyNote.D targeting banking institutions*

In addition to the spyware cases, commercial spywares (stalkerware) such as **MSpy**, **FlexiSpy**, **SpyEra**, **IkeyMonitor**, and **Cocospy** have also gained popularity. These spywares are marketed as



monitoring and surveillance tools for parents, employers, and individuals, but their potential for abuse by malicious actors raises concerns about privacy and security. Spyware can be used to monitor personal communications and track the movements of individuals, violating their privacy and potentially exposing them to danger.

The danger posed by these spyware families lies in their ability to covertly monitor and extract sensitive information from devices, potentially exposing individuals and organizations to cybercrime.

## 3.1 Remote Access Tools and ATS

### 3.1.1 RAT: Capabilities and implementation

Remote Access Tools (RATs) are becoming more and more common among banking malware. This development does not come as a surprise, considering how well it suits the needs of fraudsters: they give complete control over the infected device to criminals. Banking malware that employs such features is able to:

- **Monitor device activity** including phone calls, text messages, and Internet browsing
- Capturing **photos, audio and video** from the device's camera and microphone
- Sending and receiving **SMS messages** on behalf of the user
- **Downloading and executing** additional **malware** on the device
- **Uploading and exfiltrating data** from the device to a remote server
- **Controlling the device remotely**, including making phone calls and opening applications
- **Modifying device settings** and configurations

In modern banking malware, such features can be achieved in many different ways.

In 2021 and at the beginning of 2022 the main implementation philosophy was to delegate this part to already existing software: Families like **Hydra** and **Alien** were installing on the device **commercial** and legitimate **RAT applications**, such as TeamViewer. The Accessibility service privileges were used to setup the connection, which would then allow criminals to remotely act on the infected device.





In April 2022, with the discovery of **GodFather** and the increase of activity from **Vultur**, there was a switch that brought the RAT capabilities directly within the code base of the malware itself, albeit in the form of **third-party** libraries called by the malware during its execution.

Recently the situation has changed: currently released and active malware families, such as **Octo** and **Hook**, prefer to implement the features using **Android APIs** to interface with the **Accessibility Service** and mimic real actions on the device's UI. This allows attackers to take advantage of accessibility features and other system-level APIs to gain remote control over an infected device, making it easier to automate attacks. The use of native APIs also provides a higher level of stealth, as it makes it more difficult for security software to detect the RAT. The ability to script these RATs

is a significant advantage for attackers, as it can streamline their operations and make them more efficient.

## RAT in Android malware

### Implementation

Commercial Solutions 	Third Party Libraries 	Android Native API 
Malware installs commercial apps such as TeamViewer or AnyDesk	Malware implements interfaces with publicly available implementations of open source solutions (e.g. VNC clients)	Malware uses Accessibility Service API to create a remote session and interact with the Device's UI
<ul style="list-style-type: none"> <li>• Hydra</li> <li>• Alien</li> </ul> 	<ul style="list-style-type: none"> <li>• Vultur</li> <li>• GodFather</li> </ul>	<ul style="list-style-type: none"> <li>• Octo</li> <li>• Hook</li> </ul>

### RAT implementation categories

it is expected that the number of successful attacks using RATs and spyware will **continue to rise**, particularly in the financial sector, where attackers will seek to steal sensitive information such as login credentials and financial data.

For individuals, the impact of a RATs and spyware attack can be **devastating**. Personal information, including bank account numbers, social security numbers, and login credentials can be stolen, leading to financial loss and identity theft.

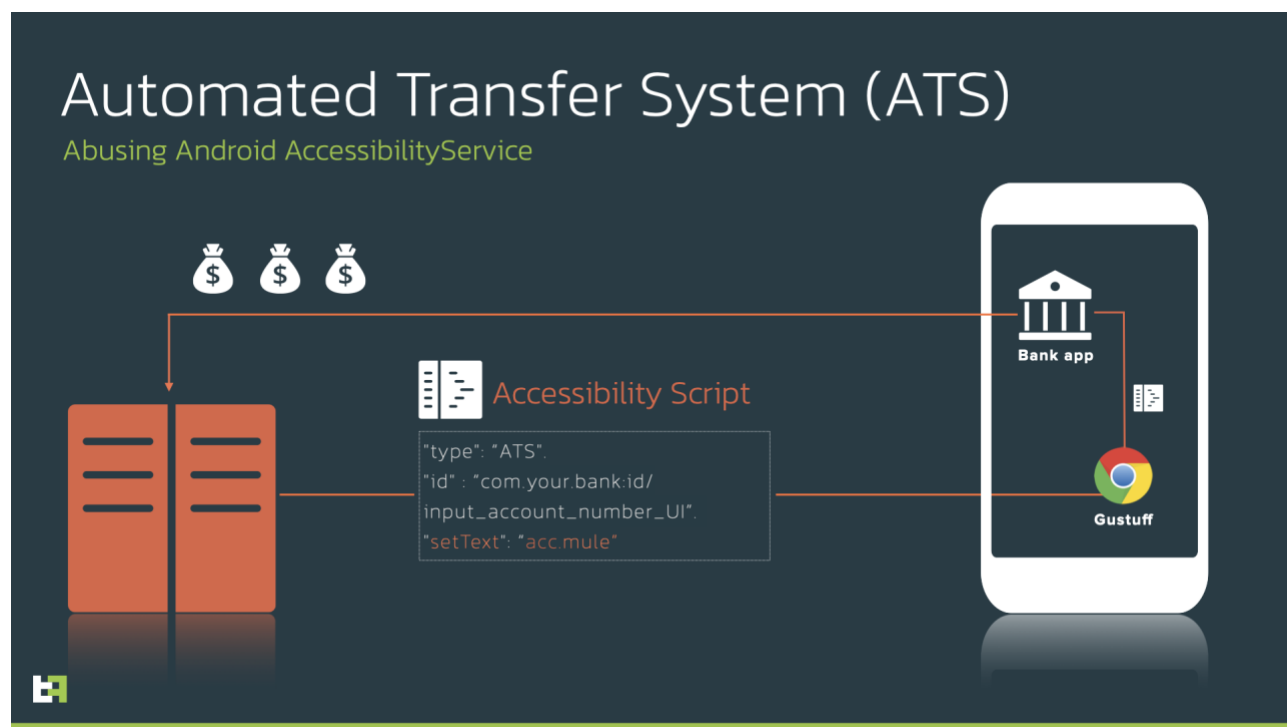
For organizations, the consequences of a RAT attack can be far-reaching and long-lasting. The loss of sensitive corporate data can lead to significant financial losses, harm to reputation, and a decline in customer trust. In addition, organizations may be subject to regulatory.

### 3.1.2 ATS: What is it?

We have discussed the increase of the number of malware families abusing Android features to perform Remote Access on infected devices. Therefore, it should not come as a surprise that paired with this trend, we are also observing an increase in families using **Automated Transfer System (ATS)** attacks.

Borrowed from the desktop malware world, this technique enables criminals to automate the whole attack chain, from the moment of infection to the transfer of funds from an infected device to an account controlled by criminals. ATS relies on traditional banking malware features to steal

credentials, together with RAT capabilities to perform all the intermediate steps required to complete the fraudulent transaction.



*ATS Script execution flow*

What sets apart families that feature ATS from ones that only implement RAT features, is the capability of performing all steps in an **automated way**, usually based on predefined actions, determined in a **programmatic way**, typically in the form of a script downloadable from the Server and updatable from actors. In this way, criminals can create ad-hoc scripts that interact with UI elements for specific procedures (like extract credentials, enable or disable features, initiate a transaction) and chain them to perform very complex operations.

# Android UI labels

AccessibilityService scripting

The slide illustrates the use of AccessibilityService scripting to interact with Android UI elements. It features a code snippet for setting text on a specific UI element and a screenshot of a mobile app interface showing a transaction confirmation screen.

**Scripting Example:**

```
@android:id=input_IBAN_account_number_UI
```

**Trojan Accessibility setText**

```
{
  "type": "money_mule",
  "id": "com.your.bank.id/
  input_IBAN_account_number_UI",
  "setText": "CZ8050513596529899771545"
}
```

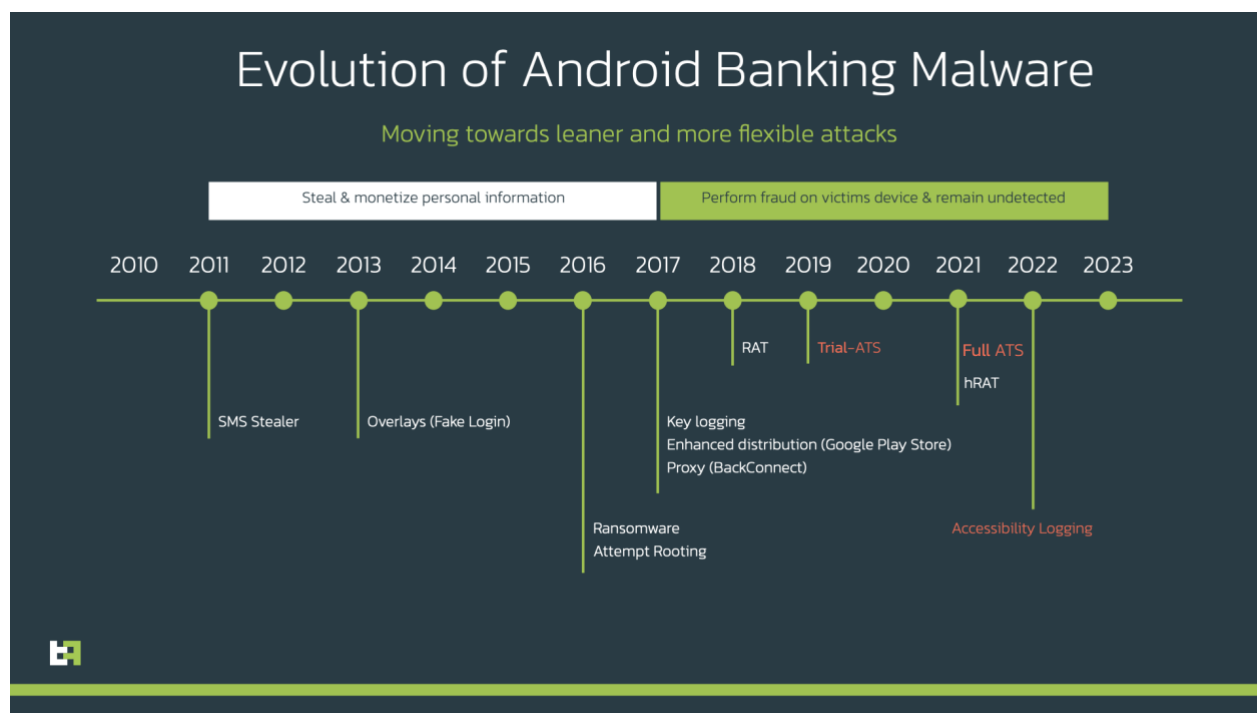
**Mobile App Interface:**

- Outgoing Transaction
- Fintory GmbH Finance Landing Page - 5.720,30 €
- Details
- Bank transfer
- #finance #fintory #design
- IBAN: DE56 3902 0000 1203 2339 39
- BIC: DUISDE33XX
- Posting Key: 153

ATS:Android UI Labes

## 3.1.3 Who features ATS

The first family to implement such a feature was **Gustuff**, which added fully developed ATS in 2019. ThreatFabric predicted this to be the direction towards which Android Banking malware was headed, and you can read more about this [on our blog](#) from 2021.



ATS Timeline



Ever since, in addition to Gustuff, which is still alive and active especially in Australia and Canada, other malware families added to their arsenal this technique.

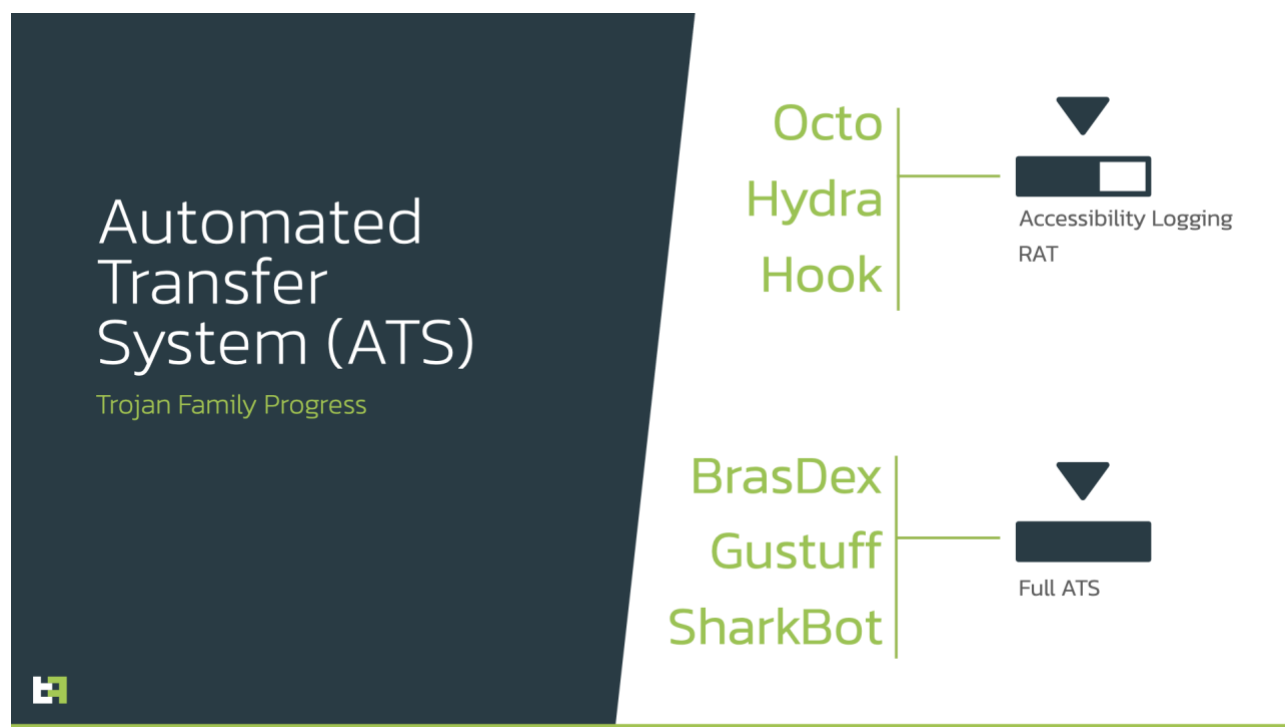
The most famous and effective in his efforts in recent times has been **SharkBot**. This malware family, active from the end of 2021, managed to wreak havoc in UK and Italy with hundreds of reported fraud attempts and hundreds of thousands of Euros stolen from online banking customers.

SharkBot uses this technique not only while attempting to perform fraud, but also during the infection chain. In some variants of its **dropper**, SharkBot uses the same ATS engine to automate the steps required to allow installation from unknown sources, accept the installation request and fully enable the downloaded application.

This action, which requires the malware to interact with different buttons based on the banking application and device manufacturer, is simply added in the configuration of the malware and included in the ATS scripts executed by SharkBot, as we previously mentioned.

More recently, we discovered a new malware family, **BrasDex**, which we discussed in depth in this [article published in December 2022](#), which used ATS scripts to automate transfers of funds using the Brazilian payment platform Pix.

In the case of BrasDex, the ATS scripts available featured the applications of all major Brazilian banking institutions, with specific details on how to handle transactions based on which kind of beneficiary information was selected by the criminal, and checks on account balances to maximize potential profits from these fraud attempts.



ATS Families

These are the most clear examples of ATS in modern banking malware. However, many other families have the potential to implement something very similar with the features already existing within their source code. Families like Octo or **Ermac/Hook** already are able to perform the **atomic**

**actions** required by ATS to complete a full attack chain.

For example, in the case of Hook/Ermac, the malware is able to execute a very long list of specific actions when it tries to extract specific information from CryptoWallet applications.

In this case, the series of actions is hardcoded in the malware itself, but if the same engine was programmed to execute a series of actions that was customizable instead, it would bridge the distance from RAT to ATS.

### 3.1.4 Dangers of ATS

The main benefit of ATS for criminals is **automation**.

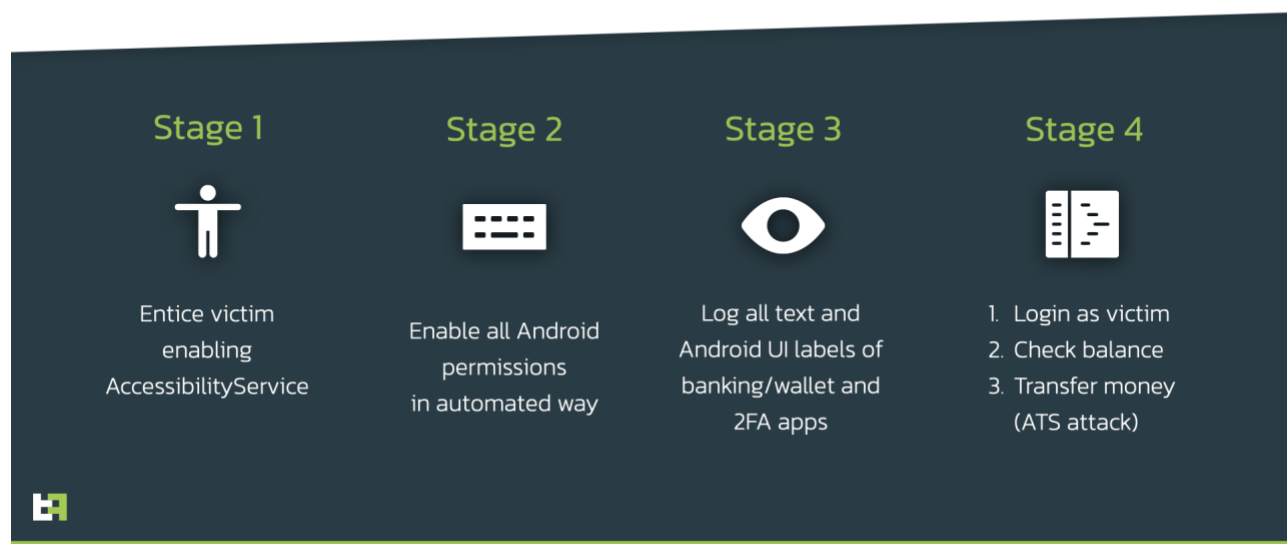
In terms of what can be achieved on a single device, ATS and RAT have the same potential. However, ATS offers criminals the potential of **scalability**, allowing TAs to operate over thousands of infected devices, without the need to individually screen and interact with each victim.

The only real trade-off for criminals is the **complexity of design** and implementation of this kind of system.

Once added and working, it adds a layer of flexibility that can only increase the threat posed by these malware families.

## Automated Transfer System (ATS)

Accessibility malware script to automate fraud



Stages of ATS

### 3.1.5 Accessibility Logging in ATS

The **rise to glory** of **Accessibility logging** in 2022 further propelled the use of ATS in modern malware.

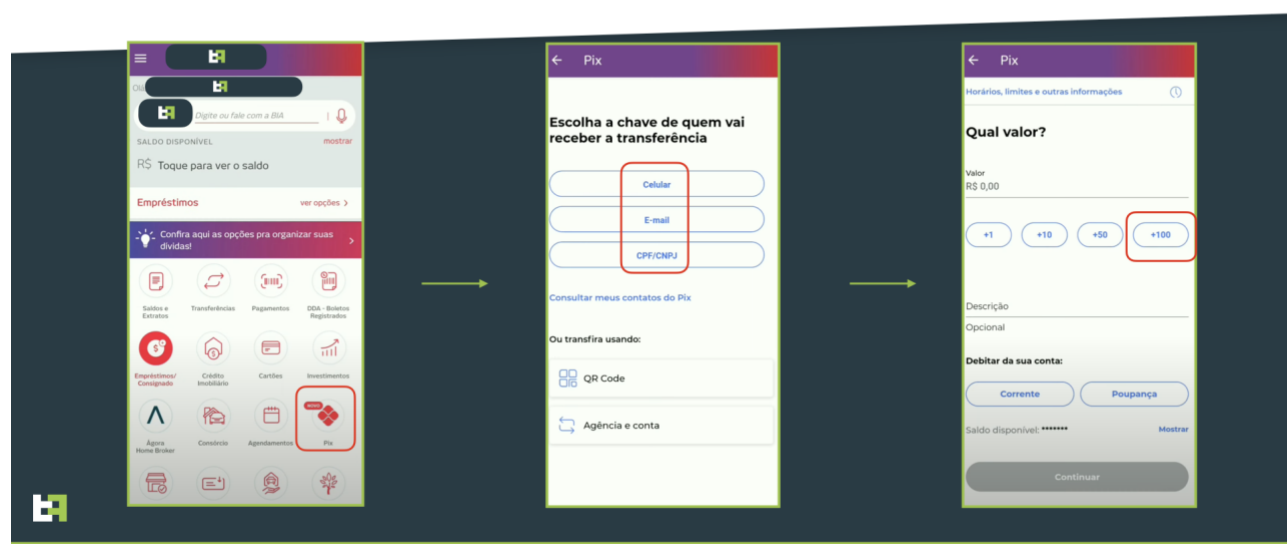
This type of logging, which is how keylogging is implemented in recent malware families, offers nicely organized information about all the **elements** of the **UI**, and can be processed and analysed by criminals, and is often used to obtain information used by ATS engines.

This sort of information includes the name, the position and the characteristics of each individual UI element. Once known, the malware can easily create scripts to interact with the application and perform the desired actions.

For example, It is often used to obtain the current balance of a bank account, in order to automatically decide the amount to transfer in the fraud attempt. This is the MO of **BrasDex**, who finds the button responsible for Pix transactions, Input the beneficiary based on the communicated data (email, phone, or fiscal number) and then, press the buttons responsible for increasing the value to the maximum funds available.

## ATS Sequence

Employed by BrasDex



*BrasDex ATS sequence abusing Pix*

With this kind of information, automation can become a very powerful tool for criminals, allowing them to design attacks which can be very hard to detect from the point of view of a fraud scoring engine.

### 3.1.6 Predictions

As we have often said in the last few years, ATS is the clear target for large malware families.

The advantages that it offers, compared to an operator-managed RAT infection, are obvious: the flexibility to programmatically manage the fraud chain, combined with the scalability opportunities



it creates, makes it an obvious choice for threat Actors. The only limitation it has is the additional development time and complexity.

Currently we are seeing this feature implemented in only a few families, and mostly in the case of private campaigns (such as BrasDex) or malware families operated by small groups of individuals (like in the cases of Gustuff and SharkBot).

In 2023 we expect an increase in the number of families that support this kind of feature. The trend has been only going up from 2019, first with Gustuff, then Sharkbot, and more recently on the other side of the Atlantic with BrasDex.



## 4. Trends and predictions

With the increasing reliance on mobile devices, particularly Android devices, the threat of malware has become a major concern for individuals and organizations alike. As technology continues to evolve, the landscape of Android malware is constantly changing, making it important to stay informed about the latest trends and predictions for the coming year.

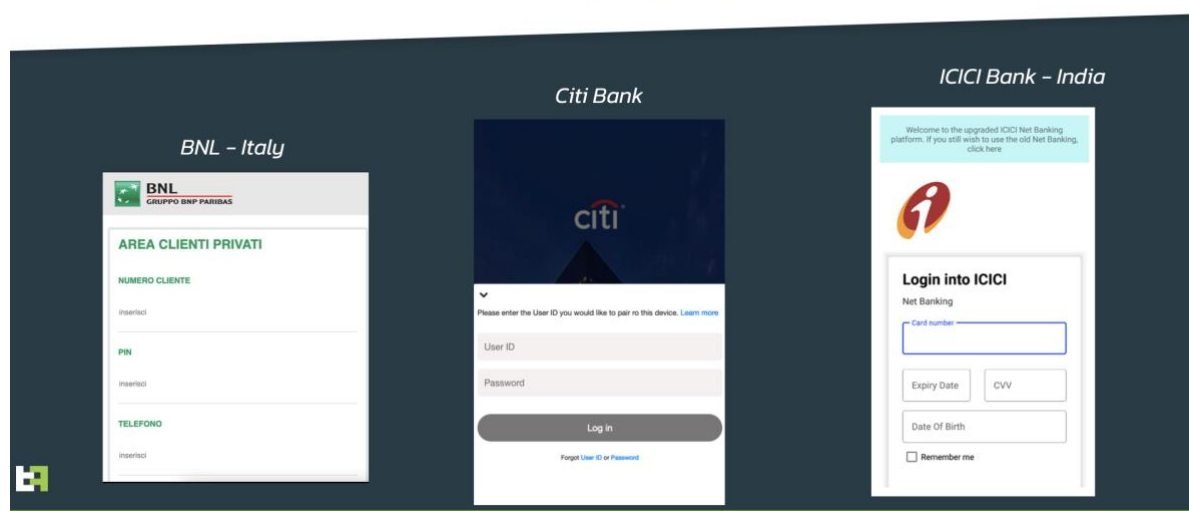
### 4.1 Phishing Attacks Targeting Financial Sector in 2022

Attackers are becoming increasingly sophisticated in their efforts to trick users into downloading malware onto their devices. The Phishing attack vector is not new, but it is still very successful and employed by actors.

As of the third quarter of 2022, OpSec Security discovered and [reported](#) that the sophistication and development of phishing attacks against the banking industry had increased to 23.2%. By utilizing **AI/Machine Learning** and customized assaults, cybercriminals were able to raise their success rates with mobile banking as a key target. As a result, banks had to contend with fresh phishing tactics aimed at their clients.

## Phishing Pages

Phishing attacks targeting multiple banks



Banking Phishing examples

Banks increased their focus on public awareness campaigns and developed new security measures, such as two-factor authentication, to counter these attacks. ThreatFabric Researchers have found several instances of these sophisticated phishing attacks, like for example a large set of malware disguising itself as rewards app that target Indian banks. Malware families like **SpyNote**, **Falcon**, and **SmsBanker** also harvest OTP from incoming SMS and collects private data using the phishing vector.

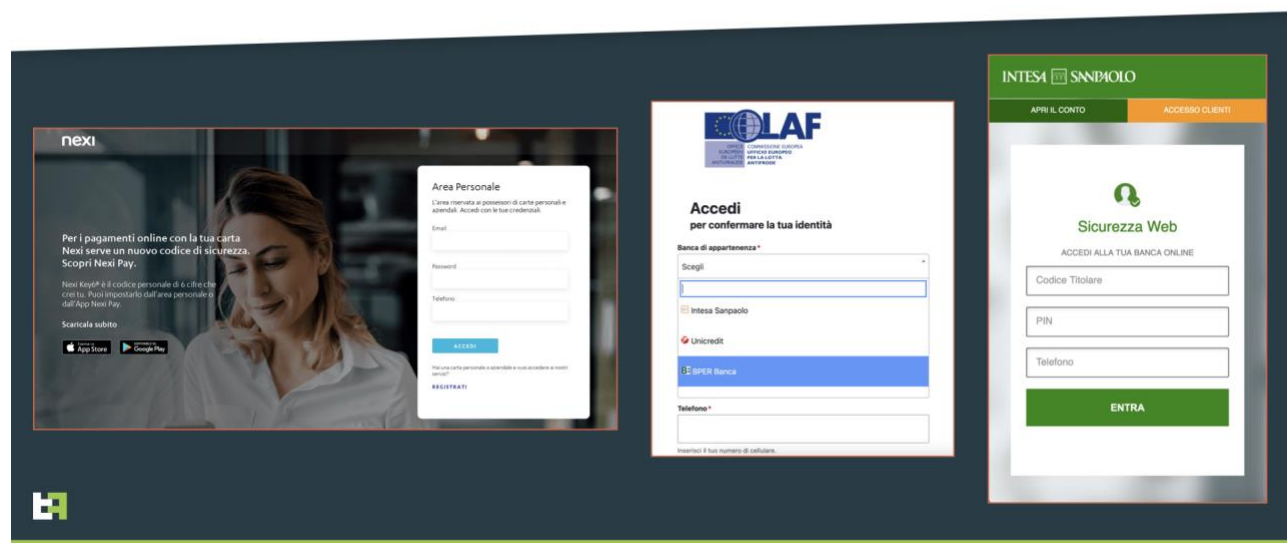
Similarly, the **Cabassous** malware family, commonly known as Flubot, and the **Alien** malware family collect **personal** and **financial** information, and have been distributed via some of the largest phishing campaigns of 2022 (in the case of Cabassous, until the takedown of the operation in May 2022).

## 4.1.1 Predictions

In 2023, it will be vital to keep a watch on malware families that use phishing as their attack vector, such as **Ermac**, **SpyNote**, and **Copybara**. These malware families are well-known for their ability to compromise devices in order to collect sensitive information while employing cutting-edge evasion strategies to avoid detection, and malware families such as Copybara are known for their telephone-oriented attack delivery (TOAD) tactics in order to gain access to victims' banking accounts via fake bank phishing pages.

# CopyBara: Phishing

## Targeting Italy



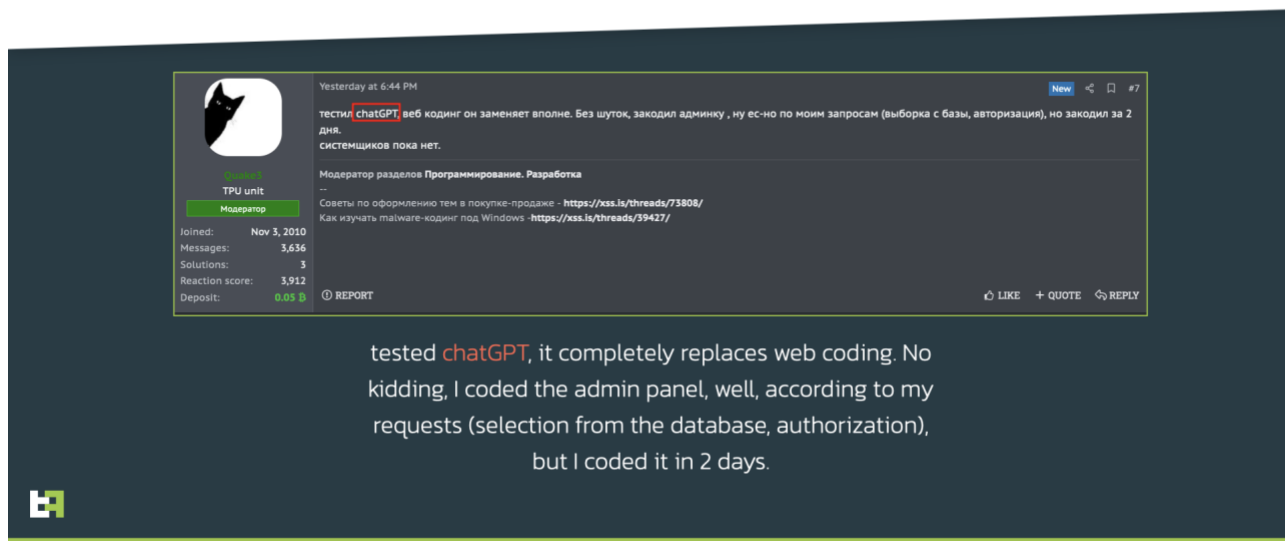
*Copybara Phishing web Pages*

Phishing attacks are adapting to use more complex and advanced strategies adopted by cybercriminals to boost success rates based on the phishing landscape observed in 2022, targeting mobile banking. With the advent of multiple **AI powered tools** in the last quarter of 2022, ThreatFabric has seen plenty of activity in hacking forums about how to use such tools to aid in the

development of both Phishing webpages as well as malware web panels.

# Phishing and AI

Actors' opinion



tested chatGPT, it completely replaces web coding. No kidding, I coded the admin panel, well, according to my requests (selection from the database, authorization), but I coded it in 2 days.

## Actors using AI to generate Web panels

Android users must be cautious and take measures to protect themselves, with only downloading apps from trustworthy stores like the Google Play Store and often upgrading both their hardware and software. Users should exercise caution when opening links in SMS or email communications and should avoid providing personal information on untrusted websites. Android users may reduce the risk of a phishing assault and safeguard their devices and data by being aware and proactive.

## 4.2 Droppers in Google Play

The use of malware droppers is also expected to increase in 2023. Malware droppers are malicious apps that are designed to download and install additional malware onto a device once they have been downloaded. These droppers can be difficult to detect and can cause significant damage to a device and its data.

Furthermore, droppers are one of the preferred distribution techniques together with TOAD (Telephone Oriented Attack Delivery) because of their high return on investment.

In 2022, the number of malware droppers targeting banks increased significantly on Google Play, the primary app store for Android devices. These droppers impersonated trustworthy banking apps, and after being installed, they downloaded malware that compromised the device and stole sensitive data.

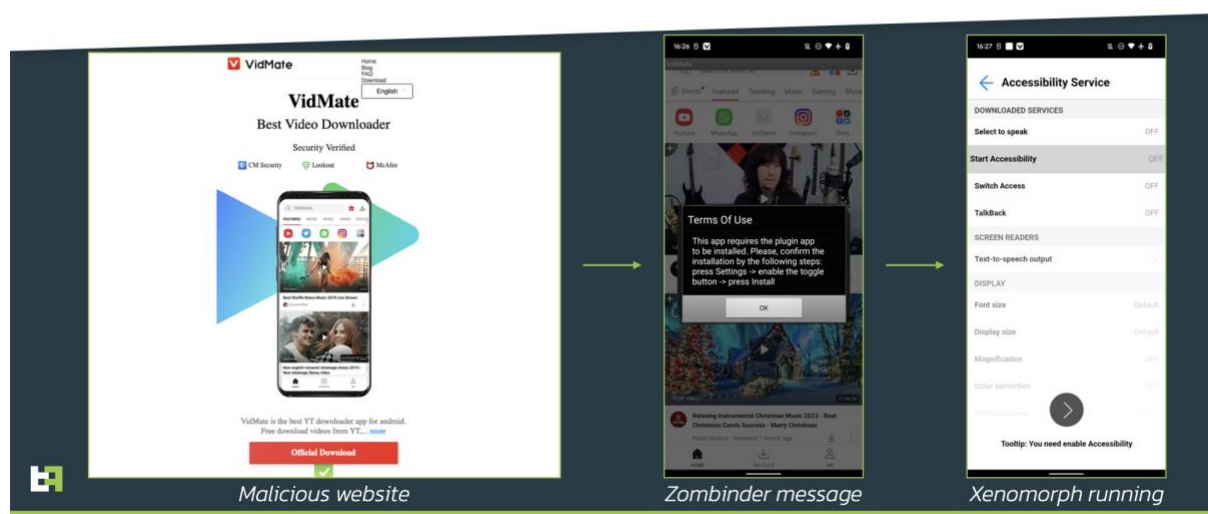
If you're interested in learning more about malware droppers in-depth, we highly recommend that you read our [blog article](#) from October 2022, which provides a thorough examination of the

evolution of droppers.

Additionally, we also discovered a new malware family named "[Zombinder](#)", that had been discovered by ThreatFabric researchers in November 2022. This malware family can "bind" its malicious code responsible for distributing banking malware to the original application's code. We found that this malware is leveraged to distribute well-known malware families including Ermac, SOVA, and the Xenomorph banking trojan.

## Zombinder

Distributing Xenomorph

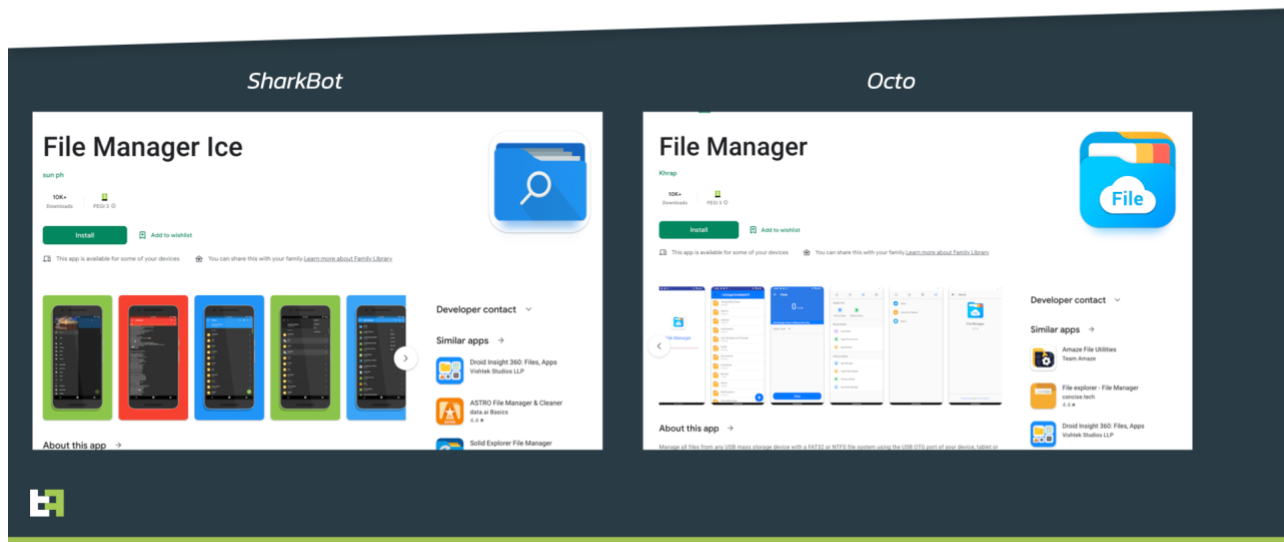


### Zombinder Execution flow

We also uncovered multiple malware droppers distributing malware families that target Italian and British banks, such as the **Octo**, rebranded and updated version of the ExobotCompact banking Trojan, and **Sharkbot**, which were transmitted through the Google Play store by disguising as File Manager applications and each having more than 5,000 installs. The application is proactively stopped from being distributed after being reported to the Google and withdrawn from the store.

# Dropper Campaigns

File Manager Campaigns in SharkBot & Octo Banking Trojan



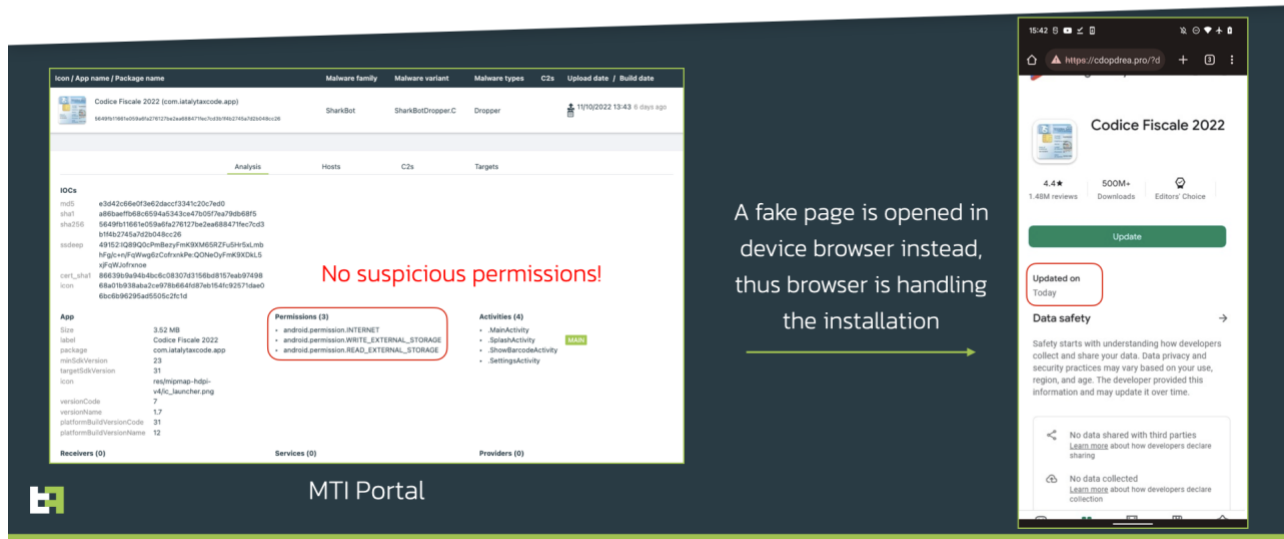
*ExobotCompact/Octo & SharkBot Dropper Campaigns*

SharkBot also used another approach in its Dropper campaigns: in one case, ThreatFabric Researchers discovered a dropper application with extremely **limited permissions required** (only Internet access and read/write permissions). In standard droppers, the application also required the permission to install another application, which is the main function of the malicious app.

However, in this case **SharkBot** used a simple redirection to a phishing page, which used the browser itself to install the malicious payload, **removing** the need to request **possibly suspicious permissions**. This approach succeeds in hiding the dropper application even further from the security and safety checks performed by AV applications as well as from the App store itself.

# SharkBot dropper

Without Installer Permission



SharkBot Dropper with limited permissions

## 4.2.1 Predictions

Although several banks have taken steps to inform their customers about these attacks and provide secure mobile banking options to protect their customers from these threats, we predict that the attackers will continue to use the most effective evasion techniques and distribution methods to distribute the droppers in the Google Play store.

## 4.3 Everything-as-a-Service (XaaS)

The rapid evolution of technology has created new and exciting opportunities for businesses and consumers alike. However, with this evolution comes new security challenges, particularly in the realm of cybercrime. In recent years, the trend of **"Everything-s-a-Service"(XaaS)** has emerged as a new threat landscape for organizations and individuals to contend with.

XaaS refers to the sale of comprehensive packages of tools and services, including pre-built malware, customized phishing pages, and access to botnets, that are designed to make it easier for less technical individuals to carry out cyberattacks. This trend is particularly concerning because it makes it easier for attackers to carry out successful attacks, regardless of their technical expertise.

In the context of Android malware, "Everything-as-a-Service"(XaaS) is an extension of the "Malware-as-a-Service"(MaaS) concept, and it provides a one-stop-shop for anyone looking to carry out cyberattacks by connecting consumers with malicious service providers. These service

providers offer their services online, often through underground forums or dark web marketplaces selling customized phishing pages, pre-built malware, and access to botnets, among other tools.

## Everything-as-a-Service

A lot of suggestions on forums

**Multiple actors provide  
installs, droppers,  
overlays, obfuscation,  
bots**

### *Everything-as-a-Service on hacking forums*

This new threat landscape is particularly concerning because it makes it easier for less technical individuals to carry out sophisticated cyberattacks. With these comprehensive packages, attackers no longer need to have the technical expertise to build their own malware or phishing pages. Instead, they can simply purchase a pre-built solution and carry out their attacks with greater ease and success.

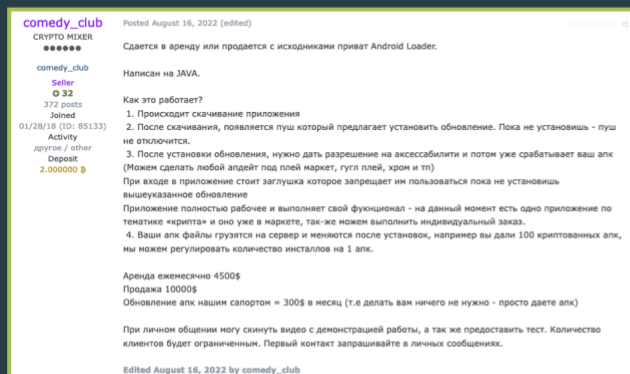
The trend of "everything-as-a-service"(XaaS) has already had a significant impact on the Android malware landscape. Actors are now specializing in different aspects, for example in terms of **distribution**, taking care of the deployment of the payload to infect the victim's device.





# Droppers on Google Play

## Dropper-as-a-Service



### Translation:

*Private Android Loader rented or sold with sources.*

*The application is fully operational and performs its functionality – at the moment there is one application on the **topic of "crypto"** and it is already in the market, we can also fulfil an **individual order**.*

*Rent monthly 4500\$*

*Sale 10000\$*

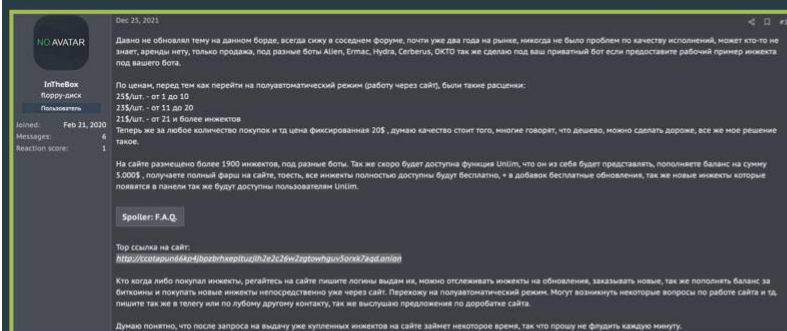
*Apk update by our support = 300\$ per month*

## Droppers-as-a-Service sold on hacking forums

In other cases, actors offer specifically designed web pages to be used by malware as **overlay**, to trick victims into revealing their PII to criminals.

# InTheBox – providing overlays

## Overlays-as-a-Service



### Translation:

*The site contains **more than 1900 overlays** for different bots. The Unlim function will also be available soon, what it will be like, top up your balance in the amount of \$ 5,000, get full stuffing on the site, that is, **all overlays will be fully available for free, + in addition free updates**, as well as new overlays that will appear in panels will also be available to Unlim users.*

## Overlays-as-a-Service sold on hacking forums





### 4.3.1 Predictions

We anticipate that the "everything-as-a-service" trend will pose a new and rising threat to both businesses and individuals in 2023. We must continue to be cautious and aggressive in our efforts to guard against cybercrime given the simplicity and success that attackers may accomplish with these all-encompassing packages.

## 4.4 Increasing the target surface

With the introduction of Accessibility logging, criminals gained access to a very large amount of information.

As previously mentioned, actors are using this feature to control balance of accounts to maximize their fraud attempts. However, this feature also opened the door to many more possibilities which were not possible before.

### 4.4.1 Seed Phrases, Emails, and Authenticator codes

**Seed Phrases** are groups of words randomly generated by cryptocurrency wallets. For all intents and purposes, they can be seen as some sort of master key to the account.

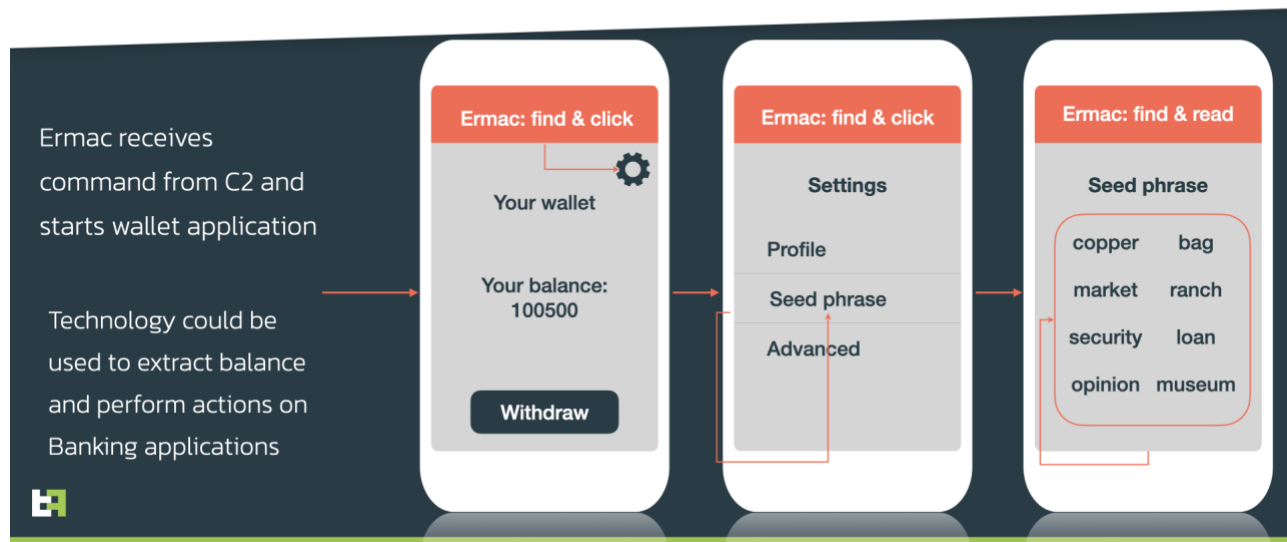
Towards the end of 2021, ThreatFabric observed for the first time a malware family, specifically Ermac, trying to exfiltrate Seed Phrases from **Cryptocurrency wallets**.

Logically, this information can be seen as credentials exfiltration. However, it differentiates itself in how it is executed. Traditionally for banking malware, credentials are stolen either via keylogging or overlay attacks. In the case of seed phrases instead, Ermac navigates through the application, using actions executed via **Accessibility Services**, to find the settings page where these phrases are stored, and then reads the UI to collect them and send them to the server.

This procedure is specific to each application, with different series of actions to be performed. In a way, it is very **similar** to the series of chained actions that can be executed in **ATS attacks**, just with the caveat of being hardcoded on the malware code itself.

# Ermac

Automated theft seed phrases



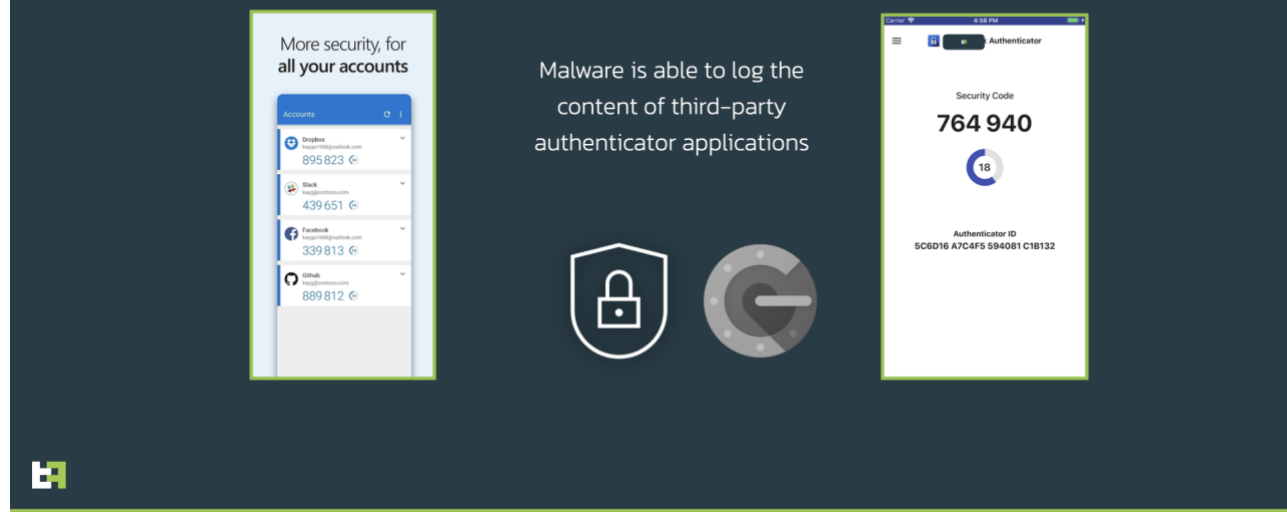
Seed Phrases Stealer Flow

In addition, the vast majority of modern banking malware can access a wide array of additional applications in order to gain even more information and power on the victim's account.

The first to appear were features to log codes within **authenticator apps**, often used to share **MFA tokens** to authorize transactions or access personal or business accounts.

## 2FA/OTP/CODE Stealer

Abusing Android AccessibilityService



MFA code stealers



More recently, Ermac also implemented the ability to launch **email clients** and log all the contents of the email account of the victim. This can be very dangerous, as this channel is often used to obtain access to any sort of account via the standard “credential reset” procedure, where users can change the login credentials of their account in case of compromised or lost passwords.

## 4.4.2 Predictions

If in 2021 the main attack MO for Android banking malware was to use overlay attacks to trick victims into revealing their credentials, it is quite clear that currently what criminals value the most is the ability to perform Accessibility logging.

With this capability, malware is effectively able to log anything that is displayed on the Device’s screen, and is not limited to a static overlay, where only credentials and Credit card numbers are usually stolen.

With Accessibility logging, criminals have access to any sort of personal information, social media, emails, OTPs, and even information about layouts of unknown applications.

We have seen a few malware families, such as Vultur or SharkBot, abandon overlays or screen streaming attacks in favour of this much more flexible solution. ThreatFabric expects this trend to continue in 2023.

## 5. Conclusions

The last year has seen a great increase in mobile fraud from criminals, connected to the continuous and clear switch in banking from desktop to **mobile**.

**Cabassous** operations overshadowed every other malware in the first half of the year. After the takedown, the crown was passed on **Hydra** and more recently to **Octo**. However, we see signs of other families, like **Hook**, joining these two families among the favourite choice when it comes to rental malware.

Banking malware has moved in the direction of **RAT**. This feature is now almost obligatory for any newly developed malware family. In addition, actors are now focusing more and more energy and efforts into automation in order to achieve **Automated Transfer Systems**, which will allow them to properly scale their criminal businesses, thanks to the gradual drift towards **Accessibility logging** as the main way to exfiltrate information from victims.

**Spyware** continues being a very dangerous threat for individuals as well as businesses. With the latest developments around **CypherRat** and **CraxsRat**, spyware has now also entered the banking fraud ecosystem, creating additional potential threat for financial institutions.

Overall, ThreatFabric sees a reduction in number of builds of individual malware families, which is the result of the abandon of the so called “spray-and-pray” approach, in favour of **more targeted and focused campaigns**, based on different distribution mechanisms which can reach a large number of potential victims, but also ensure a much larger probability of success, such as **droppers** on official app stores, **TOAD**, and heavily targeted **Phishing campaigns**.