

# Brata - a tale of three families

[threatfabric.com/blogs/brata-a-tale-of-three-families.html](https://threatfabric.com/blogs/brata-a-tale-of-three-families.html)

04 August 2022



Intro

The infosec community has a very long and undeniably bad record when it comes to naming malware families. May it be the tendency of calling anything new that appears in the wild a variation of the dreaded **<Some-string-i-found-in-the-malware>Bot**, or the necessity to note down all the different aliases used by different vendors to refer to the same malware family.

This problem is known, and often joked about among researchers: in 2022 this issue has been evident with many malware families, like Anatsa, beign known also as TeaBot or Toddler, and Cabassous, known also as Flubot.

It is not as common for the opposite problem to arise: it is infact quite rare for different malware families to share the same name. However, ThreatFabric believes this is exactly the case for what has been referred to as **Brata**.

We believe that what has been up to now categorized as Brata, is instead a conglomerate of 3 different families: Brata, AmexTroll, and Copybara.

In addition, for the for the first time we observed AmexTroll expanding its focus, from targeting only a few institutions in Italy, to featuring almost 50 different targets, among British and Australian institutions.

## The Brata saga

The first appearance of this name dates back to middle of 2019, while this malware family was reported to abuse a **CVE** in the popular instant messaging application WhatsApp to target victims in Brazil.

This malware family was also capable of keylogging data from victim's devices thanks to Accessibility Service abuse, like most modern malware families are able to do nowadays.

This campaign lasted about 6 months, and no new samples of this family were observed after the end 2019.

# Brata

Using Whatsapp CVE

The screenshot shows a list of WhatsApp updates and a security alert. The updates are for 'Atualização WA 2.5 (com.waatt25)' with various hashes. The security alert is for 'CVE-2019-3568 Detail' and is marked as 'MODIFIED'. The alert text states: 'This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.' Below the alert is a 'Current Description' section: 'A buffer overflow vulnerability in WhatsApp VOIP stack allowed remote code execution via specially crafted series of RTP packets sent to a target phone number. The issue affects WhatsApp for Android prior to v2.19.134, WhatsApp Business for Android prior to v2.19.44, WhatsApp for iOS prior to v2.19.51, WhatsApp Business for iOS prior to v2.19.51, WhatsApp for Windows Phone prior to v2.18.348, and WhatsApp for Tizen prior to v2.18.15.'

After these events, there was no mention of this malware family until the end of 2021, where reports of a new strain of Brata targeting Italy started circulating. These reports were mentioning two new variants of Brata, this time active in Europe, more specifically in Italy, with many new features and Modus Operandi.

According to the research published, the two variants were supposed subsequent iterations of the same malware family. However, ThreatFabric observed these two families being distributed simultaneously, and through different channels, throughout the first half of 2022. We also believe these **two families to be different in implementation and scope, and**

quite possibly operated by different actors. This is the reason why we do not refer to these families by the name Brata, but with two separate, different, names:

AmexTroll and Copybara.

| A tale of three families |                                |               |
|--------------------------|--------------------------------|---------------|
| Brata                    | AmexTroll                      | Copybara      |
| 2019                     | 2021-2022                      | 2021-2022     |
| Targeting in Brazil      | Targeting Italy, UK, Australia | Used in Italy |
| ODF                      | ODF                            | ODF           |

The incredible confusion within the Infosec community and financial institutions about AmexTroll and Copybara, and their alleged connections with Brata, pushed us to create this blog.

These two families share a few similarities, which led to this mistake in categorization. In addition, some leaked messages from the author of AmexTroll allegedly connect him to the development of the original Brata.

However, the differences are evident and substantiate the need to differentiate between the two, despite the possibility of having the same threat actor behind them.

## Similarities

### Basic 4 Android (B4A)

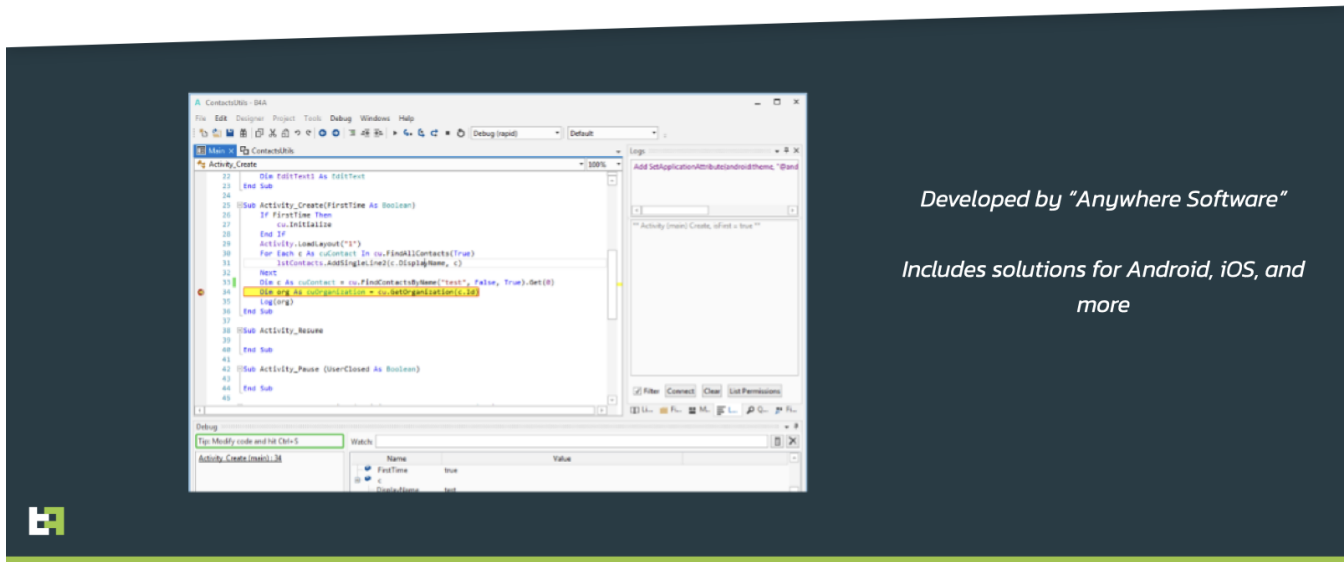
The two malware families do indeed share a few similarities in their overall design and development. Apart from being both Android Bankers, the most obvious commonality is the tools used for their development. Android natively supports two languages, Java and Kotlin. In addition, by using the JNI (Java Native Interface), developers can also interact with code written in C/C++, via a system of shared libraries.

The large majority of Android malware is developed using a combination of these two approaches. However, for both of AmexTroll and Copybara, the tool of choice is **Basic 4 Android** (from here onwards referred to as B4A).

**NOTE : ThreatFabric would like to note that B4A and the B4X suite are completely legitimate programs, and that the developers that created this project have no control over the misuse of their software.**

# Basic 4 Android

## Development Framework



B4A belongs to the **B4X suite**, developed by "Anywhere Software". Its name comes from its similarity to BASIC, despite it being an independent and proprietary language in its own. The framework relies on a combination of simple UI based designer tools and its BASIC-like language. The framework will then interpret the designs and code in the project and will create a corresponding, valid APK.

AmexTroll and Copybara are not the only malware families built using this software, despite being arguably the most advanced ones, and the appearance of such families roughly coincides with B4A becoming a free product.

In addition, this framework does not provide a built-in way to easily interact with the Accessibility services, but any average developer should be able to implement a simple bridge class to interface the framework with. In both our cases, actors seem to be using modified versions of libraries published online by other B4A users on developer forums.

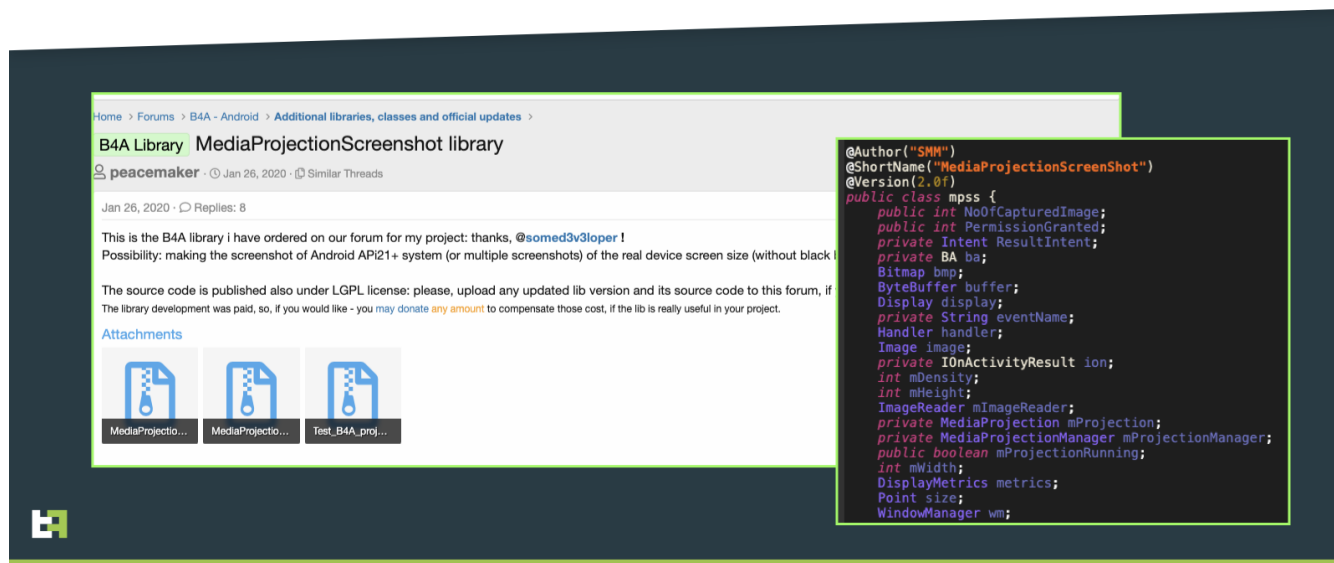
## Capabilities

In terms of capabilities, the two families do share a few common features. Most notably, they both are Android malware families targeting mostly **Italy**. In addition they also operate similarly in the way they perform **screenstreaming**:

both generate a series of screenshots every few milliseconds, which then send to the C2 to mimic a real-time video stream. In this way, operators on the other side can interact with the device remotely, allowing criminals to perform actions directly on the infected device. This feature is the key to perform On-Device Fraud (ODF) once PII's are exfiltrated, and is implemented in both cases using libraries publicly available on the B4A forum.

# Screenshot library

Used in both AmexTroll and Copybara



The image shows a screenshot of a forum thread on the B4A forum. The thread title is "MediaProjectionScreenshot library" and it was posted by user "peacemaker" on Jan 26, 2020. The thread content includes a post from "somed3v3loper" thanking the author and mentioning the library's purpose: "Possibility: making the screenshot of Android API21+ system (or multiple screenshots) of the real device screen size (without black bars)". Below the text are three attachments: "MediaProjectio...", "MediaProjectio...", and "Test\_B4A\_proj...". To the right of the forum screenshot is a code snippet in Java, enclosed in a dark box with a light border. The code defines a class "mpss" with various fields and methods, including annotations for author, short name, and version.

```
@Author("SMH")
@ShortName("MediaProjectionScreenShot")
@Version(2.0f)
public class mpss {
    public int NoOfCapturedImage;
    public int PermissionGranted;
    private Intent ResultIntent;
    private BA ba;
    Bitmap bmp;
    ByteBuffer buffer;
    Display display;
    private String eventName;
    Handler handler;
    Image image;
    private IOException ion;
    int mDensity;
    int mHeight;
    ImageReader mImageReader;
    private MediaProjection mProjection;
    private MediaProjectionManager mProjectionManager;
    public boolean mProjectionRunning;
    int mWidth;
    DisplayMetrics metrics;
    Point size;
    WindowManager wm;
}
```

Both families also sport a relatively unique feature, which allows to remotely initiate a **factory reset** on the device, potentially to disrupt investigations or clean the device from possible traces of infection. This feature is also not new, and was observed mostly in CIS malware a few years ago. However, due to its disruptiveness and debatable usefulness, it has been mostly abandoned. The feature is implemented with the same exact code in the two families. The code is the following:

```
if(accservice._manager.getEnabled()) {
    Reflection reflection0 = new Reflection();
    reflection0.Target = accservice._manager;
    reflection0.Target = reflection0.GetField("dm");
    reflection0.RunMethod2("wipeData", "0", "java.lang.int");
    return "";
}
```

However, it is worth noting that this code, as well as the code responsible for the screenshot stream, is also available online on the B4A forum, published on public threads. Considering that both families also use other code, developed and published by other users on the same forum, it is not a sufficient motive to connect the two families.

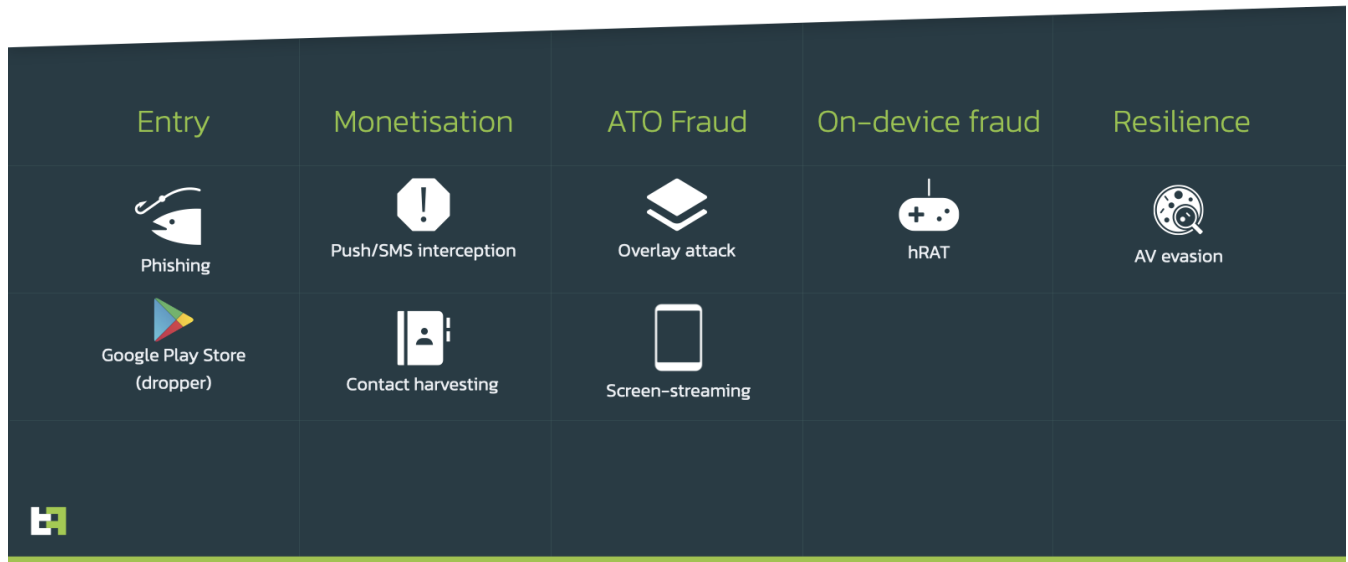
## Differences

What follows is not an extensive description of the features of the two malware families, as that has been already done by other researchers. It is a study on the differences that motivate the need for a separate categorization.

## AmexTroll

# AmexTroll Android Banking Trojan

On-Device Fraud



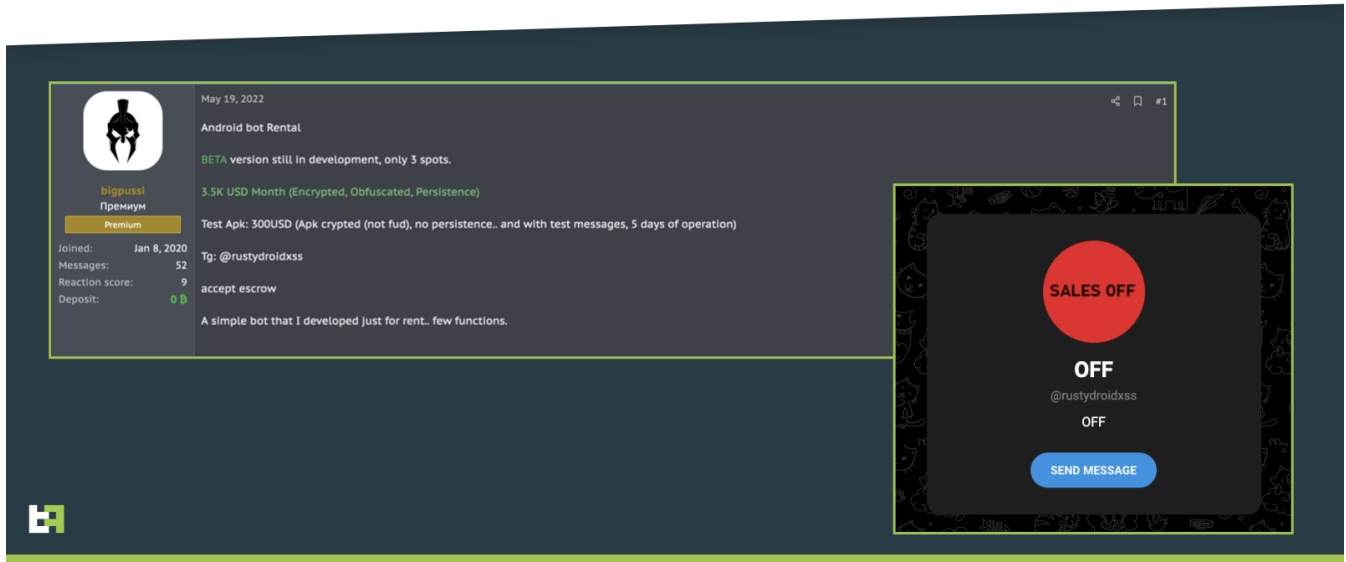
The AmexTroll family has been active since the second half of 2021, with a few initial test samples being distributed, targeting Italian institutions. The first campaign was quite limited in size, and was followed a few months after, between the end of 2021 and the beginning of 2022, by more refined campaigns, still targeting Italy, posing as an array of security related applications.

Recently, new developments brought this family on the spotlight again. The main reason behind this was the public announcement done by the actor behind its development, very likely of Brazilian origin, who put it on the market for a **beta test of a rental scheme** for his/her product. This was a notable event for this family, as up to this point it was privately ran.

The beta was able to find enough backers to proceed, as can be seen by the telegram account used to sell access to the bot:

# AmexTroll

Gone rental



After this announcement, the number of samples for this family started to increase, and so did the amount of different applications it poses as: mostly brazilian institutions as well as more generic security applications.

One feature that is specific to AmexTroll with respect to other malware families (but which incidentally exists also in the original Brata), is the “**black overlay**” feature. As the name implies, it simply consists of being able to generate a completely black overlay to display on the foreground of the device’s UI. This feature, despite being very simple, is also very dangerous for infected victims.

Here is the code responsible for this feature. As you can see, it sets up the overlay to have RGB values [0,0,0], which corresponds to black, and opacity value equal to 1. After, it calls the method responsible for overlaying the screen on the foreground of the UI.

```
public static String _open_black_overlay(String opacity) throws Exception{
    PanelWrapper panelWrapper0 = new PanelWrapper();
    panelWrapper0.Initialize(websocket_service.processBA, "");
    panelWrapper0.setColor(Colors.ARGB(((int)Double.parseDouble(opacity)), 0, 0, 0)); //
    int v = vnc_var._get_resolution(websocket_service.processBA, true);
    int v1 = vnc_var._get_resolution(websocket_service.processBA, false);
    JavaObject javaObject0 = new JavaObject();
    javaObject0.InitializeContext(websocket_service.processBA);
    javaObject0.RunMethod("criar_overlay_acess_simple", new Object[]{panelWrapper0.getObject(), ((int)0),
((int)0), v, v1});
    overlay_var._setstate_locked(websocket_service.processBA, false);
    websocket_service._reset_overlay(false);
    websocket_service._sender_sucessmessage("TRAVADO");
    return "";
}
```

The main MO of AmexTroll, which also differentiates it from Copybara, is the same overlay mechanism that is very common among other banking trojan families. Whenever the overlay is triggered, the bot automatically opens a WebView with the corresponding phishing overlay to steal the wanted PII. The implementation slightly differs from the standard used in other families due to its development cycle, but the logical steps are the same.

# AmexTroll Targets

Distributed through Google Play Store

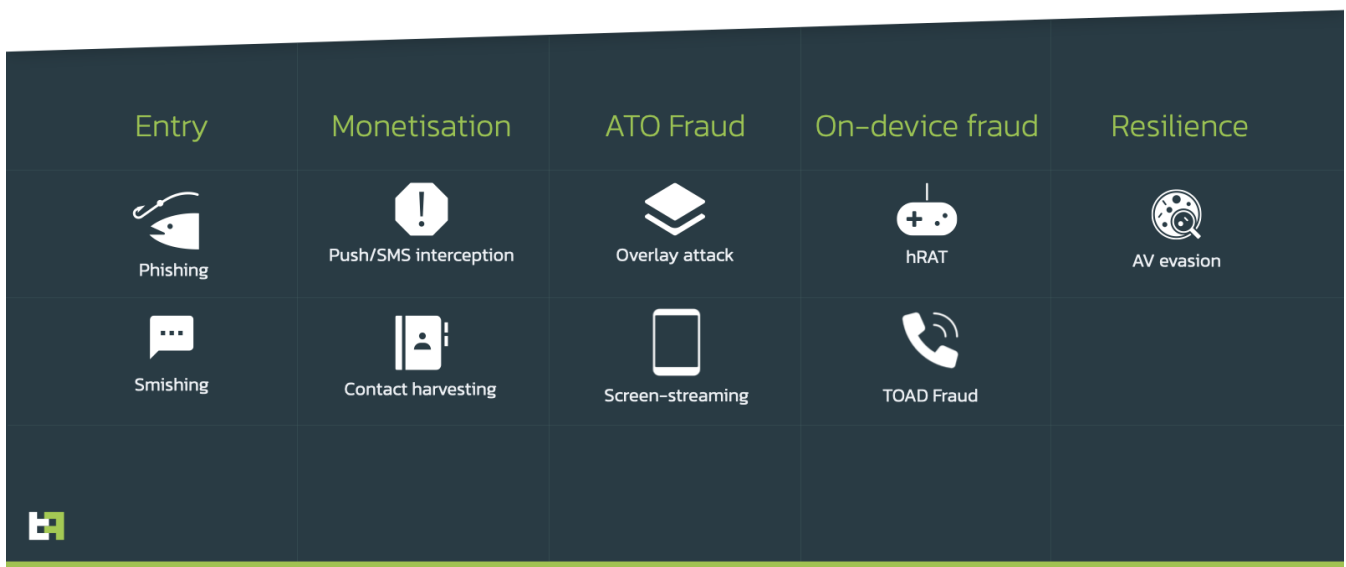


Initially the targets returned were limited, and mostly focusing on the Italian market. However, recently, a campaign that was distributed through a dropper on the **Google Play store**, was observed targeting institutions from **Australia** and **Great Britain**. The intelligence of this dropper confirm that the campaign was live for only a few days, with thousands of downloads in the aforementioned geolocations:

## Copybara

# Copybara Android Banking Trojan

On-Device Fraud



The Copybara family has also been active from the second half of 2021. The reason behind this might be found in the fact that the B4A framework became a free product in February 2020. Its campaigns came into full scope in 2022, and differ from AmexTroll for the reason that they are very focused not only on the Italian market, but also very specifically on singular



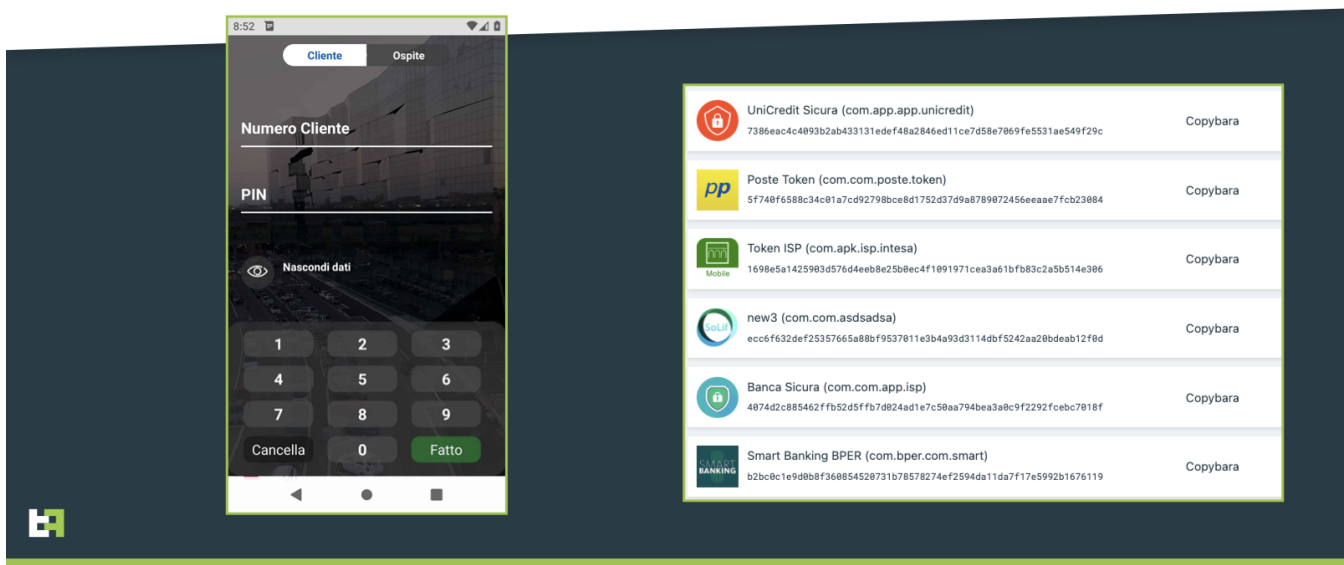
institutions.

The malware itself, similarly to AmexTroll, is able to create a **remote connection with the C2** and allow criminals to perform **On-Device Fraud** on the infected device. However, Copybara greatly differs in the way that it obtains PII's.

Similarly to AmexTroll, it features an overlay mechanism, but in this case it is **specific** to the application it is posing as (in a way that is very similar to what malware use to do before the use of accessibility services became prevalent). ThreatFabric has found samples posing as a variety of Italian institutions; however, the overlay is consistently the same within this set of applications.

# Copybara

Overlay screen



Newer variants of this family also introduced **additional modules** and **APKs**, which add functionalities to the malware itself. The main Copybara application is able to download an external module, capable of performing Accessibility event logging, a feature that is extremely important when implementing On-Device Fraud, as it allows criminal to have a full visibility and actionability on all the UI elements on the victim's devices, as well as allowing to implement a very inclusive keylogging mechanism.

```
if(acs.GetIsStringTypeText().toString().length() > 0 && accessibilityNodeInfo0 != null &&
(var1.getClassName().equals("android.widget.EditText"))) {
    if(accessibilityNodeInfo0.getActionList().contains(AccessibilityNodeInfo.AccessibilityAction.ACTION_SET_TEXT))
    {
        Bundle var4 = new Bundle();
        var4.putCharSequence("ACTION_ARGUMENT_SET_TEXT_CHARSEQUENCE", acs.GetIsStringTypeText().toString());
        accessibilityNodeInfo0.performAction(0x200000, var4);
    }
    else if(TextUtils.isEmpty(accessibilityNodeInfo0.getText())) {
        accessibilityNodeInfo0.performAction(0x8000);
    }
    else if(!accessibilityNodeInfo0.getText().toString().contains(acs.GetIsStringTypeText().toString()))
    {
        accessibilityNodeInfo0.performAction(0x8000);
    }
}

acs.IsStringTypeText("");
}
```

Combined with the additional modules, copybara utilizes some companion apps that deal with SMS monitoring and refer to the same C2 as the main malware. These apps are used to retrieve possible 2FA tokens from banks, as well as monitoring even further the device. These are also distributed through the same web phishing channels as Copybara.

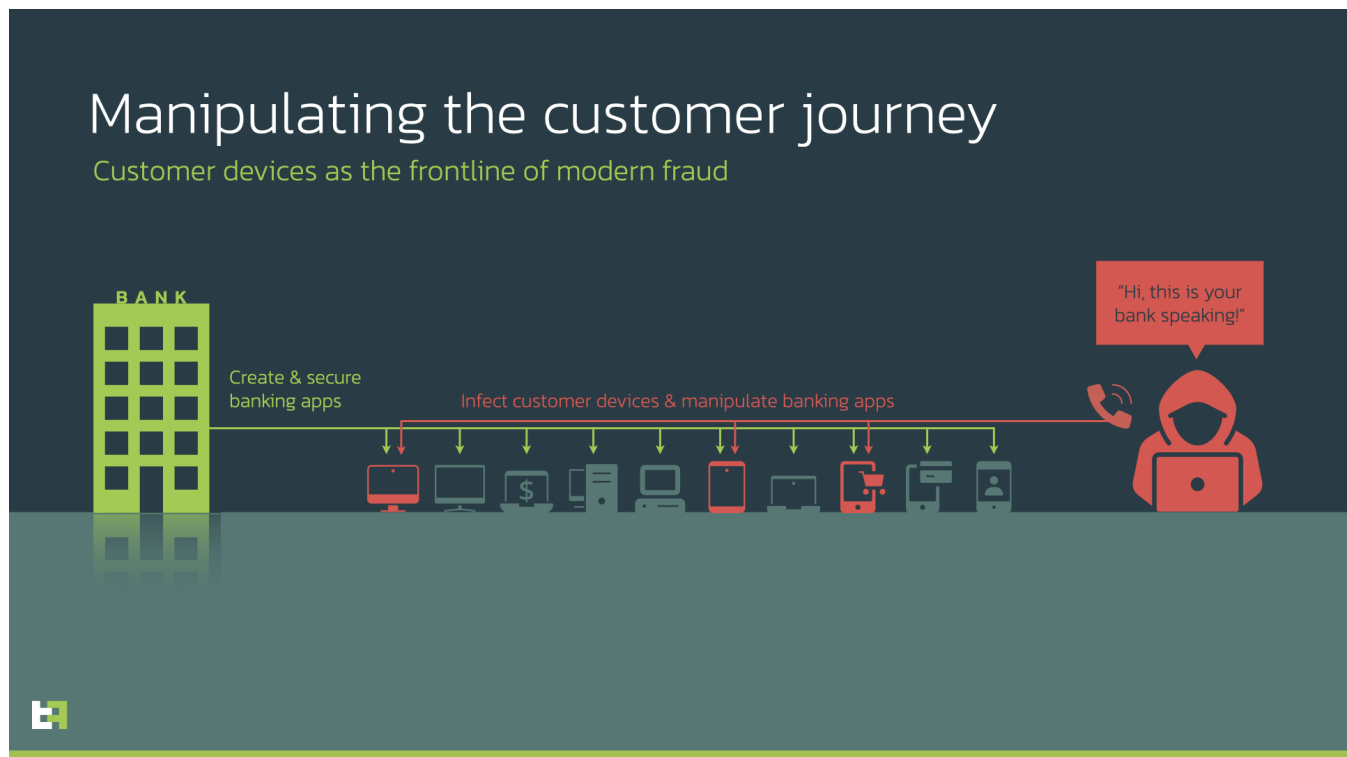
However, the real strength of Copybara lies within the criminal group behind it. The lack of flexibility in this malware family is greatly balanced by the care and precision of its **social engineering** approach.

Copybara, by virtue of being privately run, is able to heavily rely on **TOAD (Telephone-oriented attack delivery)**, which involves operators calling the victim to convince them to install and grant all the necessary permissions to function. This is the main difference between this family and AmexTroll, and one of the main reasons why ThreatFabric feels very confident in differentiating these two families.

Users may be very skeptical about applications downloaded from the Web (problem that AmexTroll tackles by using droppers on Google Play Store to gain trust from users).

Copybara is distributed via **SMiShing**. Victims receive a SMS from their bank with a link, followed by a **call by the operator** to guide them through the process. The additional step of being called by an operator adds credibility to the operation, encouraging users to install the malware with the promise of being safer and more protected.

This approach is very effective, and justifies the nature of the malware itself. The group behind Copybara works with much more limited numbers of infections, due to the necessity of an operator interaction with the victim. However, this step also ensures a much higher success rate. This also may be the reason why this family is heavily focused on the Italian market. This approach requires to heavily tailor the process to the banking institution targeted, so it makes sense for criminals to focus on one language at a time.



## Conclusions

The mobile malware landscape is continuously evolving and mobile users are continuously facing new and different threats. In 2022, ThreatFabric has observed a strong shift towards On-Device Fraud. AmexTroll and Copybara confirm this trend, while adding their own flair to the standard Android Banking Malware features, one being technical addition to make infection stealthier and more effective, the other relying on the human aspect of phishing, to literally coach victims into correctly infecting their own devices.

ThreatFabric expects to see more from both of these families, which are alive and active at the time of writing this blog.

## 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](mailto:sales@threatfabric.com).

## Appendix

### Brata Samples

| App name             | Package name           | SHA-256  |
|----------------------|------------------------|--|
| Atualização WhatsApp | com.da9d84d1           | 22a841da43ced0f2bb829780a4aa6a2ffaeb56d2a5e98d2f1bd62e1b8d70b967 |
| com.helper.android   | com.helper.android     | 91ab6e70655abdef8e79eae0d83c02246037e2fc168eec956192fac4fcecea6  |
| Vivo Internet Gratis | com.vivointernetgratis | 4c57c5eae5a1bae1a50beed28affdf722c89416886e5eda8088a06771cc29c8  |
| Atualização WA 2.5   | com.waatt25            | fa816c631249922539eeeb3e8f73d3ef4ea997ab729751adebcea3d0de32a63b |

### AmexTroll Samples

| App name                     | Package name          | SHA-256  |
|------------------------------|-----------------------|--|
| A Shield Auth                | horse.house.homer     | f530c66fb1f7ac5e2e9a89c1f410e498dc59eecbec8bae29a9f69ab3dc7ce86c |
| 1. Itau Modulo Segurança     | koala.viber.vip       | 02aa9061b47762ce1627d38195097c0e791864004e509598269ffa8fb2e25103 |
| 1. TEST APP KOALA (Test app) | malware.malware.virus | 1032b42c859c747bcc159b75366c3325869d3722f5673d13a7b06633245ebf32 |
| 1. SICUREZZA ANTISPAM        | koala.kerox.vip       | 38952ffe92afea051cea6de48b765274f5344ae2add07820995340faf546e220 |

### Copybara Samples

| App name         | Package name          | SHA-256  |
|------------------|-----------------------|--|
| Banca Sicura     | com.com.app.isp       | 4074d2c885462ffb52d5ffb7d024ad1e7c50aa794bea3a0c9f2292fceb7018f  |
| Token ISP        | com.apk.isp.intesa    | 1698e5a1425903d576d4eeb8e25b0ec4f1091971cea3a61bfb83c2a5b514e306 |
| UniCredit Sicura | com.app.app.unicredit | 7386eac4c4093b2ab433131edef48a2846ed11ce7d58e7069fe5531ae549f29c |
| Banca Sicura     | com.banca.sicura.app  | 94f1a33d4f3bd94f65f8969f288fe01a198952c17e52c9e86e4047222d45f0ce |

### AmexTroll targets

| PackageName            | AppName  |
|------------------------|----------|
| au.com.bankwest.mobile | Bankwest |

| <b>PackageName</b>                      | <b>AppName</b>                           |
|---|--|
| au.com.commbank.commbiz.prod            | CommBiz                                  |
| au.com.cua.mb CUA                       | Mobile Banking                           |
| au.com.hsbc.hsbc australia              | HSBC Australia                           |
| au.com.macquarie.banking                | Macquarie Mobile Banking                 |
| au.com.mebank.banking                   | ME Bank                                  |
| au.com.nab.mobile                       | NAB Mobile Banking                       |
| au.com.newcastlepermanent               | NPBS Mobile Banking                      |
| au.com.rams.RAMS                        | myRAMS                                   |
| au.com.suncorp.rsa.suncorpsecured       | Suncorp Secured                          |
| au.com.suncorp.SuncorpBank              | Suncorp Bank                             |
| au.com.ubank.internetbanking            | UBank Mobile Banking                     |
| co.zip                                  | Zip - Shop Now, Pay Later                |
| com.anz.android.gomoney                 | ANZ Australia                            |
| com.anz.transactive.global              | ANZ Transactive - Global                 |
| com.bankofqueensland.boq                | BOQ Mobile                               |
| com.bendigobank.mobile                  | Bendigo Bank                             |
| com.commbank.netbank                    | CommBank                                 |
| com.fusion.banking                      | Bank Australia app                       |
| com.fusion.beyondbank                   | Beyond Bank Australia                    |
| com.greater.Greater                     | Greater Bank                             |
| com.hsbc.hsbcnet                        | HSBCnet Mobile                           |
| com.virginmoney.cards                   | Virgin Money Credit Card                 |
| org.banking.bom.businessconnect         | Bank of Melbourne Business App           |
| org.banking.bsa.businessconnect         | BankSA Business App                      |
| org.banking.stg.businessconnect         | St.George Business App                   |
| org.banksa.bank                         | BankSA Mobile Banking                    |
| org.bom.bank                            | Bank of Melbourne Mobile Banking         |
| org.stgeorge.bank                       | St.George Mobile Banking                 |
| org.westpac.bank                        | Westpac Mobile Banking                   |
| org.westpac.col                         | Westpac Corporate Mobile                 |
| co.uk.Nationwide.Mobile                 | Nationwide Banking App                   |
| com.barclaycardus                       | Barclays US                              |
| com.cooperativebank.bank                | The Co-operative Bank                    |
| com.grppl.android.shell.CMBllloydsTSB73 | Lloyds Bank Mobile Banking: by your side |

| <b>PackageName</b>                              | <b>AppName</b>                                |
|---|---|
| com.grppl.android.shell.halifax                 | Halifax: the banking app that gives you extra |
| com.ie.capitalone.uk                            | Capital One UK                                |
| com.nearform.ptsb                               | permanent tsb                                 |
| com.rbs.mobile.android.natwest                  | NatWest Mobile Banking                        |
| com.revolut.revolut                             | Revolut - Get more from your money            |
| tsb.mobilebanking                               | TSB Bank Mobile Banking                       |
| uk.co.hsbc.hsbcukmobilebanking                  | HSBC UK Mobile Banking                        |
| uk.co.metrobankonline.mobile.android.production | Metro Bank                                    |
| uk.co.santander.santanderUK                     | Santander Mobile Banking                      |
| uk.co.tsb.newmobilebank                         | TSB Mobile Banking                            |
| it.carige                                       | Carige Mobile                                 |

## Copybara targets

---

### Bank

Unicredit Banca

---

Banca Intesa

---

BNP

---

BPER Banca

---

Poste Italiane