Cerberus - A new banking Trojan from the underworld

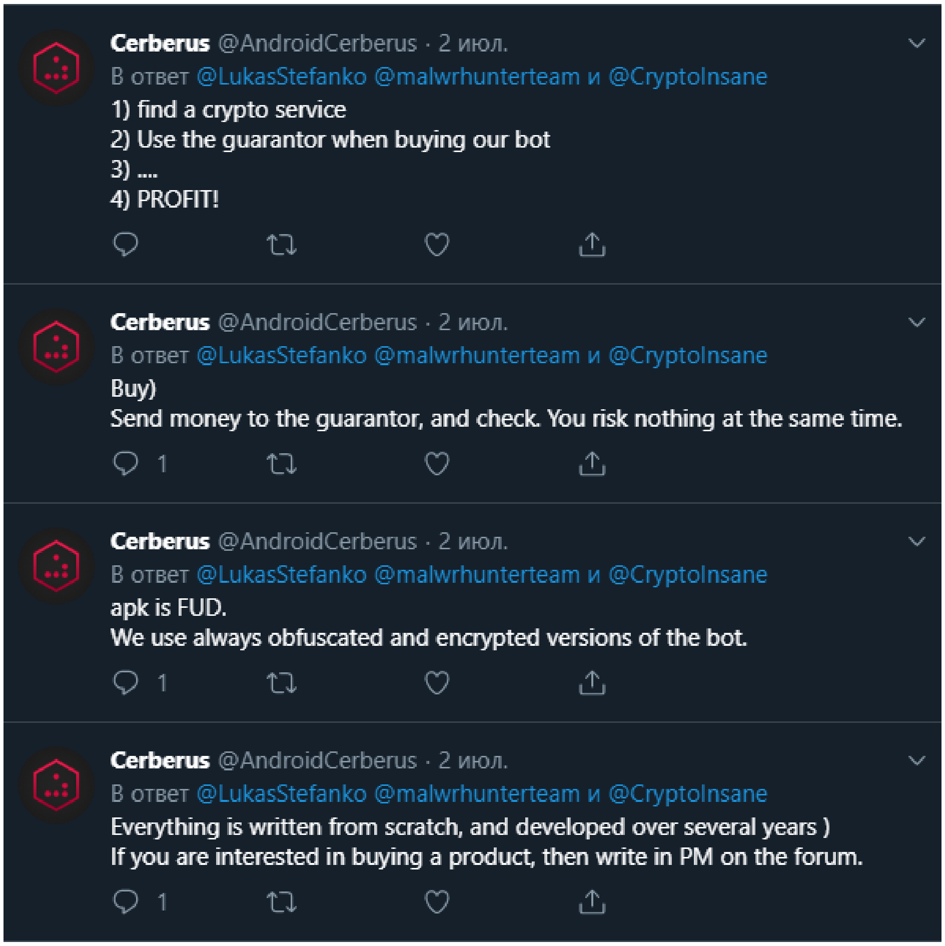
August 2019

Intro

In June 2019, ThreatFabric analysts found a new Android malware, dubbed “Cerberus”, being rented out on underground forums. Its authors claim that it was used for private operations for two years preceding the start of the rental. They also state that the code is written from scratch and is not using parts of other existing banking Trojans unlike many other Trojans that are either based completely on the source of another Trojan (such as the leaked Anubis source code that is now being resold) or at least borrow parts of other Trojans. After thorough analysis we can confirm that Cerberus was indeed not based on the Anubis source code.

One peculiar thing about the actor group behind this banking malware is that they have an “official” twitter account that they use to post promotional content (even videos) about the malware. Oddly enough they also use it to make fun of the AV community, sharing detection screenshots from VirusTotal (thus leaking IoC) and even engaging in discussions with malware researchers directly.

The following screenshot shows tweets from their advertisement campaign:



Cerberus @AndroidCerberus · 2 июл.
В ответ @LukasStefanko @malwrhunterteam и @CryptoInsane
1) find a crypto service
2) Use the guarantor when buying our bot
3) ....
4) PROFIT!

Cerberus @AndroidCerberus · 2 июл.
В ответ @LukasStefanko @malwrhunterteam и @CryptoInsane
Buy)
Send money to the guarantor, and check. You risk nothing at the same time.

Cerberus @AndroidCerberus · 2 июл.
В ответ @LukasStefanko @malwrhunterteam и @CryptoInsane
apk is FUD.
We use always obfuscated and encrypted versions of the bot.

Cerberus @AndroidCerberus · 2 июл.
В ответ @LukasStefanko @malwrhunterteam и @CryptoInsane
Everything is written from scratch, and developed over several years)
If you are interested in buying a product, then write in PM on the forum.

That unusual behavior could be explained by the combination of the need for attention and a probable lack of experience.

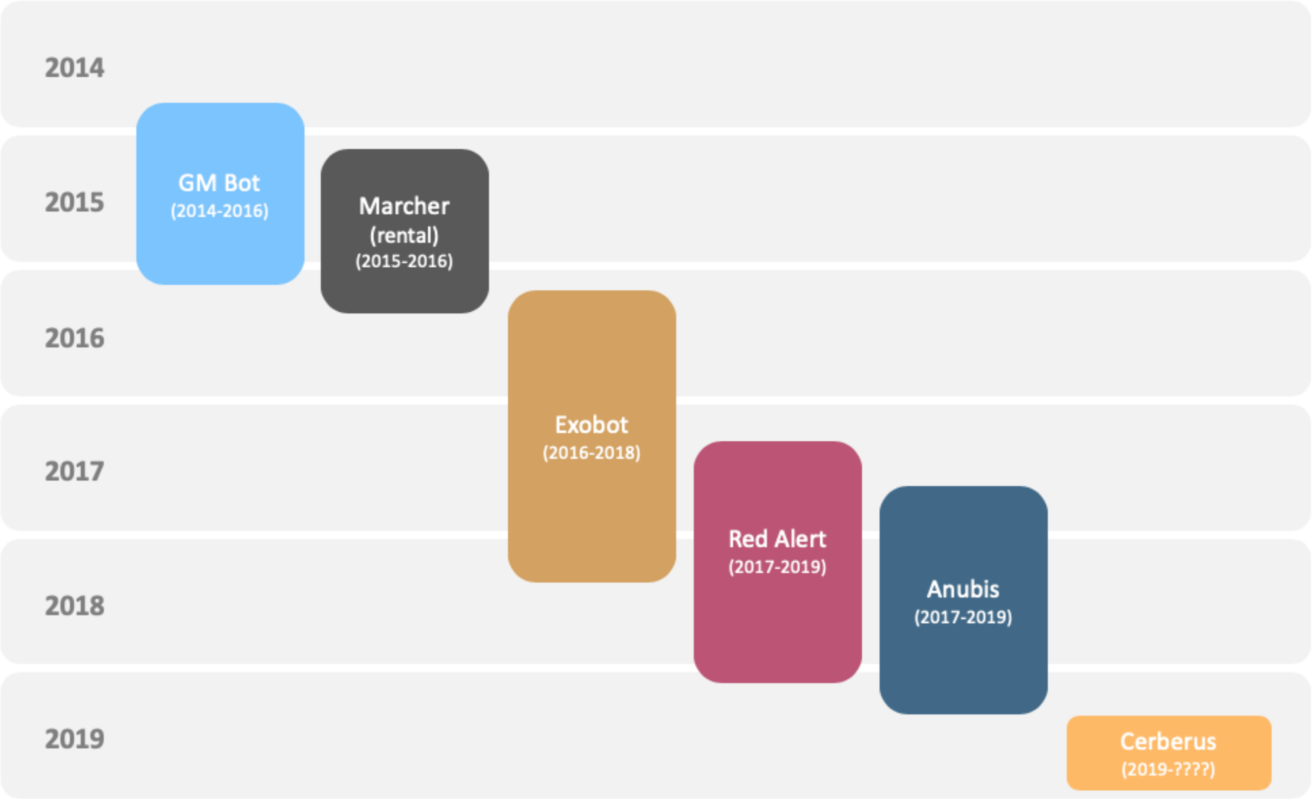
What is sure is that the gap in the Android banking malware rental business left open after the rental of the Anubis 2 and RedAlert 2 Trojans ended provides a good opportunity for the actors behind Cerberus to grow their business quickly.

The Android banking Trojan rental business

Rental of banking Trojans is not new. It was an existing business model when computer-based banking malware was the only form of banking malware and has shifted to the Android equivalent a few years later.

The life span of Android banking malware is limited to either the will of its author(s) to support it or the arrest of those actors. This malware-life-cycle has been observed to reoccur every few years, bringing new malware families into light. Each time a rented malware reaches the end of its life it provides the opportunity for other actors a to take over the malware rental market-share.

As visible on following chart, the lifespan of many well-known rented Android bankers is usually no more than one or two years. When the family ceases to exist a new one is already available to fill the void, proving that the demand for such malware is always present and that therefore Cerberus has a good chance to survive.



After the actor behind RedAlert 2 decided to quit the rental business, we observed a surge in Anubis samples in the wild. After the Anubis actor was allegedly arrested and the source code was leaked there was also huge increase in the number of Anubis samples found in the wild, but the new actors using Anubis have no support or updates.

Due to this Cerberus will come in handy for actors that want to focus on performing fraud without having to develop and maintain a botnet and C2 infrastructure.

Analysis of evasion techniques

Along with the standard payload and string obfuscation, Cerberus uses a rather interesting technique to prevent analysis of the Trojan.

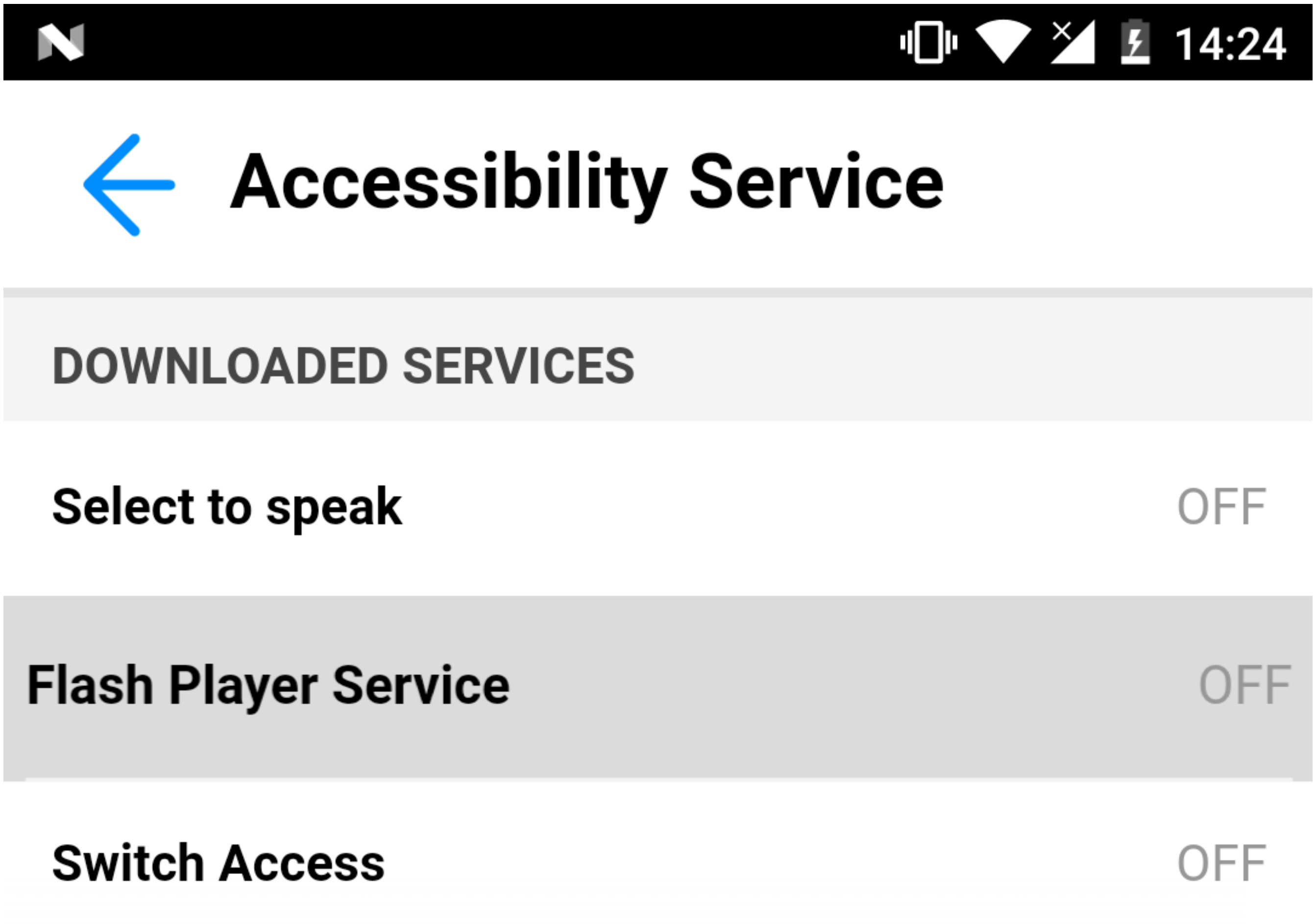
Using the device accelerometer sensor it implements a simple pedometer that is used to measure movements of the victim. The idea is simple - if the infected device belongs to a real person, sooner or later this person will move around, increasing the step counter. The Trojan uses this counter to activate the bot - if aforementioned step counter hits the pre-configured threshold it considers running on the device to be safe. This simple measure prevents the Trojan from running and being analyzed in dynamic analysis environments (sandboxes) and on the test devices of malware analysts.

The code responsible for this verification is shown in the following snippet:

```
...
this.sensorService.registerListener(this, this.accelerometer, 3);
Sensor localSensor = sensorEvent.sensor;
this.sensorService.registerListener(this, localSensor, 3);
if(localSensor.getType() == 1) {
    float\[\] values = sensorEvent.values;
    float Gx = values\[0\];
    float Gy = values\[1\];
    float Gz = values\[2\];
    long timestamp = System.curTimeMillis();
    if(timestamp - this.previousTimestamp > 100L) {
        long interval = timestamp - this.previousTimestamp;
        this.previousTimestamp = timestamp;
        if(Math.abs(Gx + Gy + Gz - this.curGx - this.curGy - this.curGz)
            / (((float)interval)) * 10000f > 600f) {
            this.increaseStepCount();
        }

        this.curGx = Gx;
        this.curGy = Gy;
        this.curGz = Gz;
    }
}
...
if(Integer.parseInt(
    this.utils.readConfigString(arg7, this.constants.step)) < this.constants.limit) {
    goto skip;
}
```

How it works

When the malware is first started on the device it will begin by hiding its icon from the application drawer. Then it will ask for the accessibility service privilege as visible in the following screenshot:



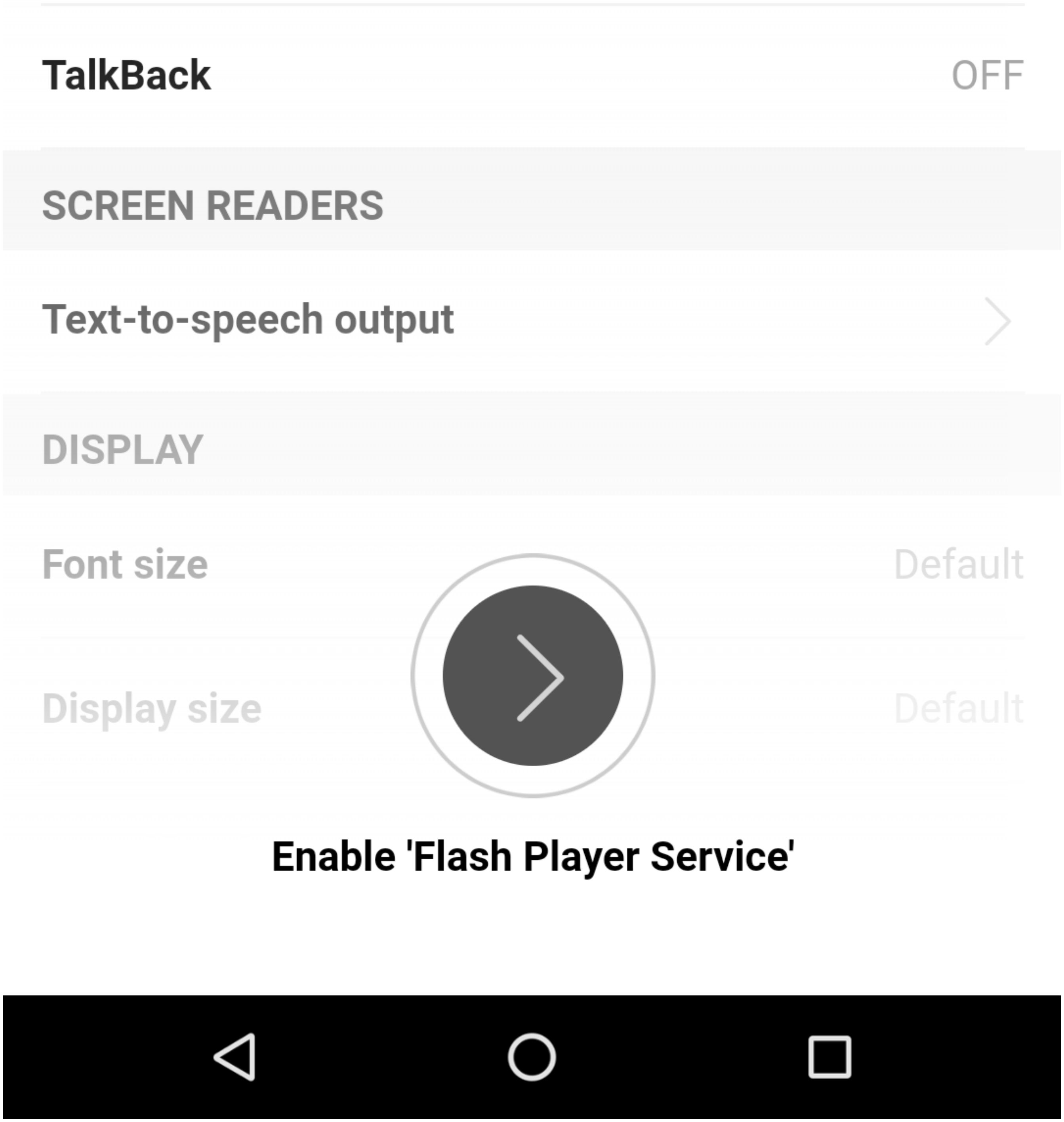
Accessibility Service

DOWNLOADED SERVICES

Select to speak OFF

Flash Player Service OFF

Switch Access OFF



TalkBack OFF

SCREEN READERS

Text-to-speech output

DISPLAY

Font size Default

Display size Default

Enable 'Flash Player Service'

After the user grants the requested privilege, Cerberus starts to abuse it by granting itself additional permissions, such as permissions needed to send messages and make calls, without requiring any user interaction. It also disables Play Protect (Google’s preinstalled antivirus solution) to prevent its discovery and deletion in the future. After conveniently granting itself additional privileges and securing its persistence on the device, Cerberus registers the infected device in the botnet and waits for commands from the C2 server while also being ready to perform overlay attacks.

The commands supported by the analyzed version of the Cerberus bot are listed below. As can be seen, the possibilities offered by the bot are pretty common.

Command	Description
push	Shows a push notification. Clicking on thenotification will result in launching a specified app

Command	Description
startApp	Starts the specified application
getInstallApps	Gets the list of installedapplications on the infected device
getContacts	Gets the contact names and phone numbers from the addressbook on the infected device
deleteApplication	Triggers the deletion of the specified application
forwardCall	Enables call forwarding to the specified number
sendSms	Sends a text message with specified text from the infecteddevice to the specified phone number
startInject	Triggers the overlay attack against the specified application
startUssd	Calls the specified USSD code
openUrl	Opens the specified URL in the WebView
getSMS	Gets all text messages from the infected device
killMe	Triggers the kill switch for the bot
updateModule	Updates the payload module

Cerberus features

Cerberus malware has the same capabilities as most other Android banking Trojans such as the use of overlay attacks, SMS control and contact list harvesting. The Trojan can also leverage keylogging to broaden the attack scope. Overall, Cerberus has a pretty common feature list and although the malware seems to have been written from scratch there does not seem to be any innovative functionality at this time. For example, some of the more advanced banking Trojans now offer features such as a back-connect proxy, screen-streaming and even remote control.

Cerberus embeds the following set of features that allows itself to remain under the radar and successfully perform attacks:

- Overlaying: Dynamic (Local injects obtained from C2)
- Keylogging
- SMS harvesting: SMS listing
- SMS harvesting: SMS forwarding
- Device info collection
- Contact list collection
- Application listing
- Location collection
- Overlaying: Targets list update
- SMS: Sending
- Calls: USSD request making
- Calls: Call forwarding
- Remote actions: App installing
- Remote actions: App starting
- Remote actions: App removal
- Remote actions: Showing arbitrary web pages
- Remote actions: Screen-locking
- Notifications: Push notifications
- C2 Resilience: Auxiliary C2 list
- Self-protection: Hiding the App icon
- Self-protection: Preventing removal
- Self-protection: Emulation-detection

- Architecture: Modular

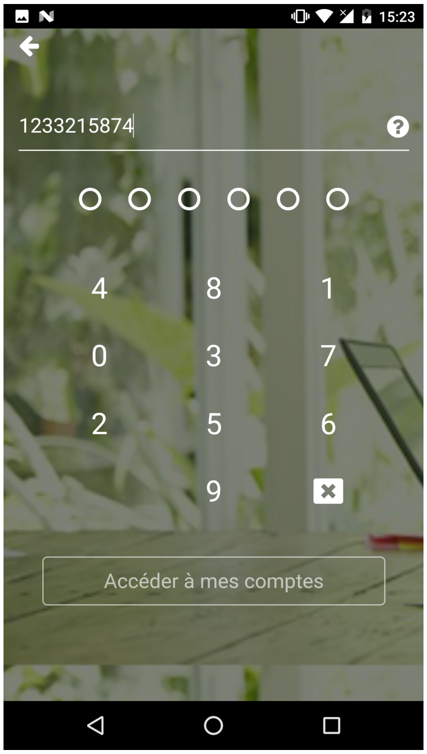
Overlay attack

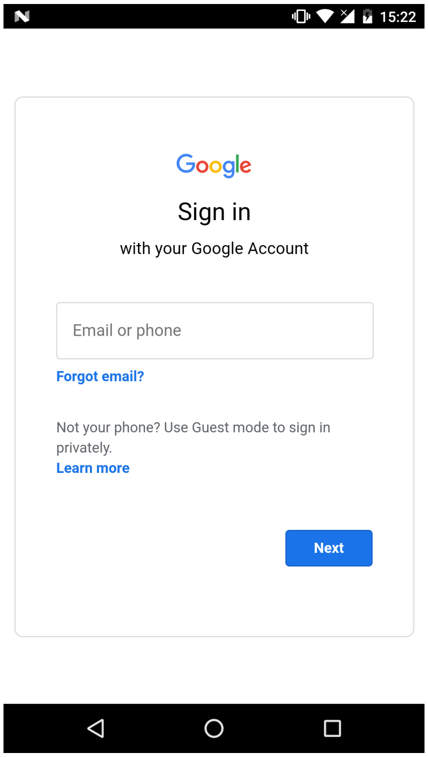
Most Android banking Trojans use overlay attacks to trick the victim into providing their personal information (such as but not limited to: credit card information, banking credentials, mail credentials) and Cerberus is no exception. In this particular case, the bot abuses the accessibility service privilege to obtain the package name of the foreground application and determine whether or not to show a phishing overlay window, as shown in the following code snippet:

```
this.foregroundAppPackage = accesibilityEvent.getPackageName().toString();

...

String target = this.strings.empty;
if(this.strings.CC_apps.contains(this.foregroundAppPackage)) {
    target = this.strings.grabbCC;
}
else if(this.strings.MAIL_apps.contains(this.foregroundAppPackage)) {
    target = this.strings.grabMails;
}

try {
    Utils utils = this.utils;
    String v1_10 = target.isEmpty() ? this.foregroundAppPackage : target;
    if(utils.readConfigString(this, v1_10).length() > 10) {
        JSONObject config = new JSONObject();
        config.put(this.strings.params, this.strings.startViewInject);
        config.put(this.strings.packageAppStart, this.foregroundAppPackage);
        config.put(this.strings.nameInject, target);
        config.put(this.strings.packageProject, this.getPackageName());
        config.put(this.strings.packageView, InjectActivity.class.getCanonicalName(););
        Utils utils1 = this.utils;
        utils1.callModule(this, config.toString());
    }
}
catch(Exception e) {
    ...
}
```

Targets

Some examples of phishing overlays are shown below. They exist in two types: the credentials stealers (first 2 screenshots) and the credit card grabbers (last screenshot).




Google

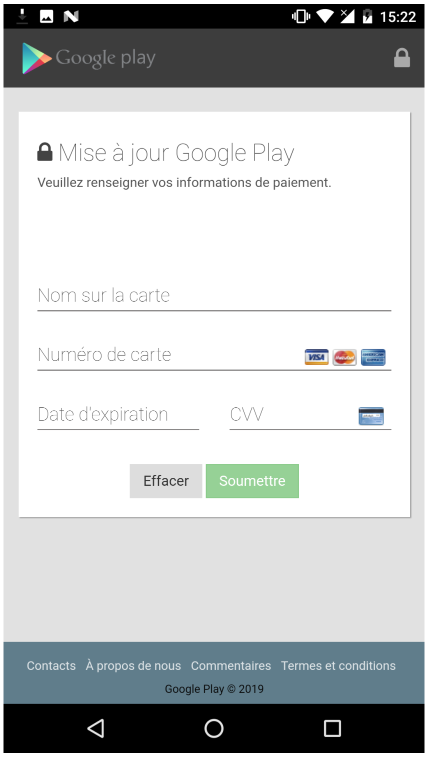
Sign in

with your Google Account

Email or phone

Forgot email?

Not your phone? Use Guest mode to sign in privately.
Learn more


Mise à jour Google Play

Veuillez renseigner vos informations de paiement.

Nom sur la carte

Numéro de carte

Date d'expiration

CVV

Contacts À propos de nous Commentaires Termes et conditions

Google Play © 2019

The only active target list observed in the wild is available in the appendix and contains a total of 30 unique targets.

It is interesting to observe that the actual target list contains:

- 7 French banking apps
- 7 U.S. banking apps
- 1 Japanese banking app
- 15 non-banking apps

This uncommon target list might either be the result of specific customer demand, or due to some actors having partially reused an existing target list.

Conclusion

Although not yet mature enough to provide the equivalent of a full-blown set of Android banking malware features (such as RAT, RAT with ATS (Automated Transaction Script), back-connect proxy, media streaming), or providing an exhaustive target list, Cerberus should not be taken lightly.

Due to the current absence of maintained and supported Android banking Malware-as-a-Service in the underground community, there is a certainly demand for a new service. Cerberus is already capable to fulfill this demand. In addition to the feature base it already possesses and the money that can be made from the rental, it could evolve to compete with the mightiest Android banking Trojans. Next to the features, we expect the target list to be expanded to contain additional (banking) apps in the near future.

Knowledge of the threat landscape and implementation of the right detection tools remains crucial to be able to protect yourself from fraud; Cerberus is yet a new Trojan active in the wild!

Mobile Threat Intelligence

Our threat intelligence solution – MTI, provides the context and in-depth knowledge of the past and present malware-powered threats in order to understand the future of the threat landscape. Such intelligence, includes both the strategic overview on trends and the operational indicators to discern early signals of upcoming threats and build a future-proof security strategy.

Client Side Detection

Our online fraud detection solution – CSD, presents financial institutions with the real-time overview on the risk status of their online channels and related devices. This overview provides all the relevant information and context to act upon threats before they turn into fraud. The connectivity with existing risk or fraud engines allows for automated and orchestrated, round the clock fraud mitigation.

Appendix

Samples

Some of the latest Cerberus samples found in the wild:

App name	Package name	SHA 256 hash
Flash Player	com.uxlgtsvfdc.zipvwntdy	728a6ea44aab94a2d0ebbccbf0c1b4a93fbd9efa8813c19a88d368d6a46b4f4f
Flash Player	com.ognbsfhszj.hqpquokjdp	fe28aba6a942b6713d7142117afdf70f5e731c56eff8956ecdb40cdc28c7c329
Flash Player	com.mwmnfwt.arhkrgajn	ffa5ac3460998e7b9856fc136ebcd112196c3abf24816ccab1fbae11eae4954c
Flash Player	com.wogdjywtwq.oiofvpzpxyo	6ac7e7ed83b4b57cc4d28f14308d69d062d29a544bbde0856d5697b0fc50cde4
Flash Player	com.hvdnaiujzwo.fovzeukzywfr	cfd77ddc5c1ebb8498c899a68ea75d2616c1c92a0e618113d7c9e5fcc650094b
Flash Player	com.gzhlubw.pmevdiexmn	3f2ed928789c200e21fd0c2095619a346f75d84f76f1e54a8b3153385850ea63

Target list

The actual observed list of mobile apps targeted by Cerberus contains a total of 30 unique applications. This list is expected to expand:

Package name	Application name
com.android.vending	Play Market
com.boursorama.android.clients	Boursorama Banque
com.caisseepargne.android.mobilebanking	Banque
com.chase.sig.android	Chase Mobile
com.clairmail.fth	Fifth Third Mobile Banking
com.connectivityapps.hotmail	Connect for Hotmail
com.google.android.gm	Gmail
com.imo.android.imoim	imo free video calls and chat

Package name	Application name
com.infonow.bofa	Bank of America Mobile Banking
com.IngDirectAndroid	ING
com.instagram.android	Instagram
com.konylabs.capitalone	Capital One® Mobile
com.mail.mobile.android.mail	mail.com mail
com.microsoft.office.outlook	Microsoft Outlook
com.snapchat.android	Snapchat
com.tencent.mm	WeChat
com.twitter.android	Twitter
com.ubercab	Uber
com.usaa.mobile.android.usaa	USAA Mobile
com.usbank.mobilebanking	U.S. Bank - Inspired by customers
com.viber.voip	Viber
com.wf.wellsfargomobile	Wells Fargo Mobile
com.whatsapp	WhatsApp
com.yahoo.mobile.client.android.mail	Yahoo Mail – Organized Email
fr.banquepopulaire.cyberplus	Banque Populaire
fr.creditagricole.androidapp	Ma Banque
jp.co.rakuten_bank.rakutenbank	楽天銀行 -個人のお客様向けアプリ
mobi.societegenerale.mobile.lappli	L’Appli Société Générale
net.bnpparibas.mescomptes	Mes Comptes BNP Paribas
org.telegram.messenger	Telegram