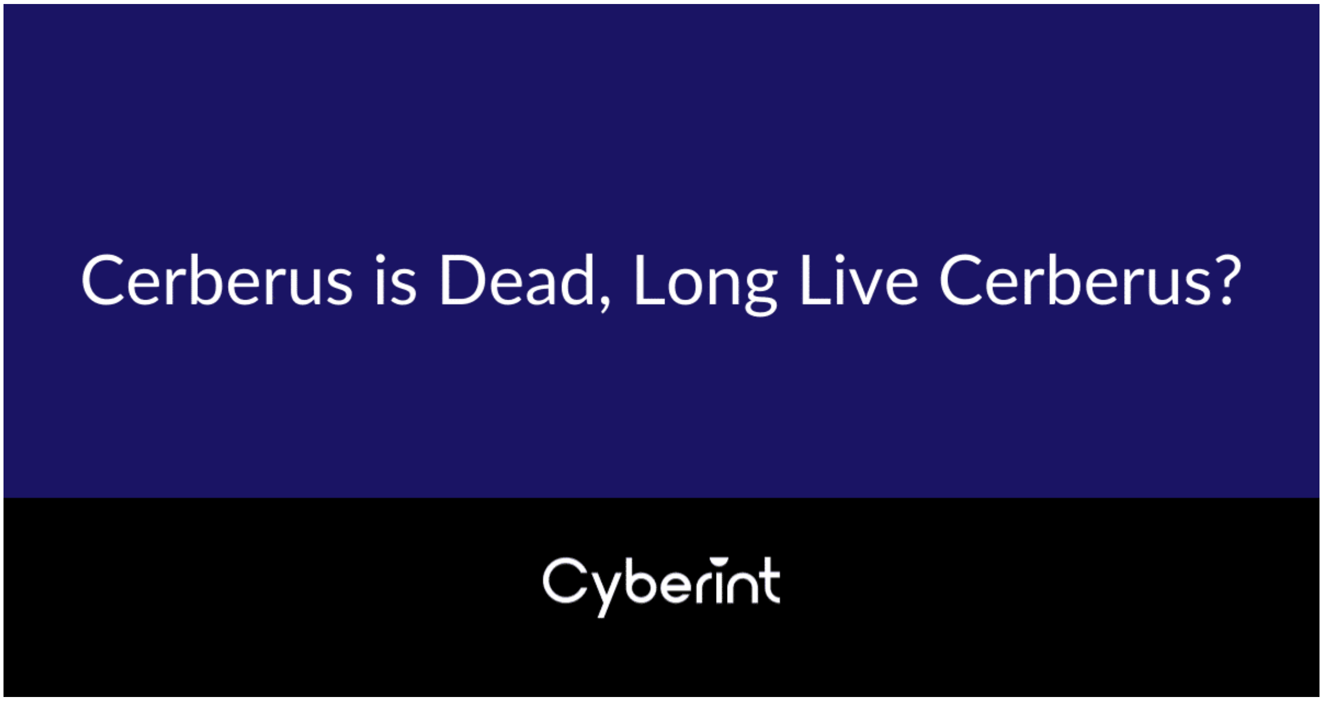
Cerberus is Dead, Long Live Cerberus?

blog.cyberint.com/cerberus-is-dead-long-live-cerberus

November 5, 2020



Executive Summary

This blog provides an overview of the situation surrounding the release of the source code, and supplementary ‘injection’ files, for the Android banking trojan ‘Cerberus’. In addition to the source code for two versions of the malicious application along with the control panel being freely available on various underground forums, over two hundred injection files, those being HTML pages that mimic the look of legitimate Android apps, have been distributed and could allow the theft of credentials and/or payment card data.

Given that the current threat from Cerberus was countered by Google Play Protect, Google’s own Android antimalware solution, other threat actors may act on comments from Cerberus’ creators to restore the threat, or simply use the source code to create, or further develop, their own Android threats.

Recent reports indicate that Cerberus is now targeting Android users in Russia as well as countries within the Commonwealth of Independent States (CIS), suggesting that some ‘less-patriotic’ threat groups have modified the source code and removed these previously defined ‘safe countries’. Other than this activity, no other regions have been specifically identified at increased risk.

As time elapses and threat actors gain a better understanding of the released code, others may seek to utilize it, or the injection pages, in their own threats or campaigns. This is especially true given the availability of a Cerberus ‘installation service’, costing just USD 300, that could allow a lower-sophistication threat actor to gain access to a working Cerberus control panel with Android application package (APK) builder for a fraction of its former cost.

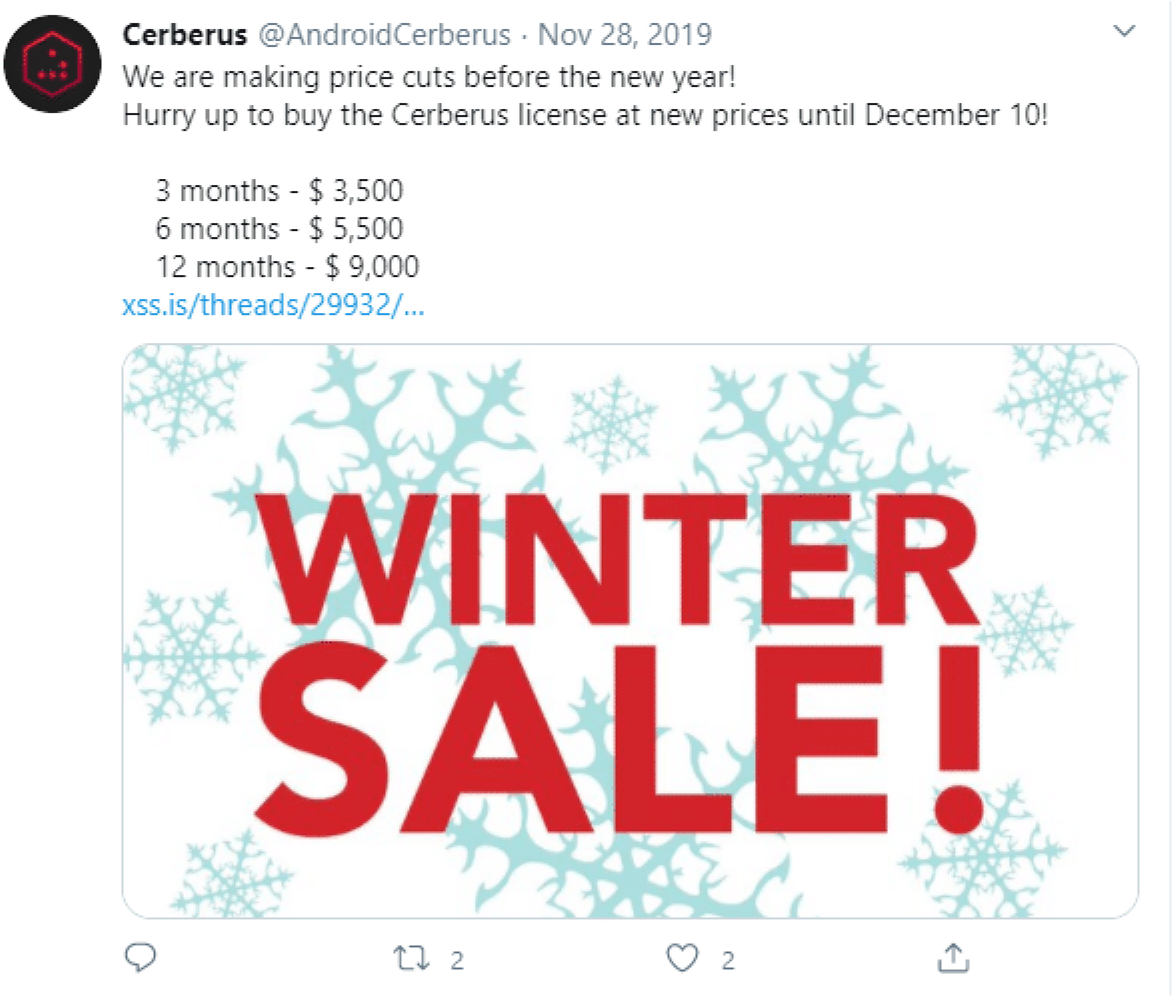
Introduction

Believed to have been in development for some time and used privately for around two years prior to being first observed by cybersecurity researchers in June 2019, Cerberus is an Android banking trojan that was available via a malware-as-as-service (Maas) offering as advertised on underground forums (Figure 1).

Figure 1 – Cerberus advertisement banners (Bottom: Updated for Cerberus V2)

As is common for threats of this nature, Cerberus supports various capabilities out-of-the-box, such as the ability to interact with, and steal data from, a compromised device including contacts, SMS interception and call forwarding, as well as selling addons in the form of ‘injections’ that allow credentials and/or payment card data to be stolen from specific legitimate applications.

Reportedly earning the creators at least USD 10,000 a month during its peak, not withstanding any ill-gotten gains made from stolen data, the MaaS model used to rent access to Cerberus’ infrastructure was, when not discounted (Figure 2), available in three packages (USD 4,000 for 3 months, USD 7,000 for 6 months and USD 12,000 for one year of access) in addition to injections reportedly selling for USD 4,000 each.



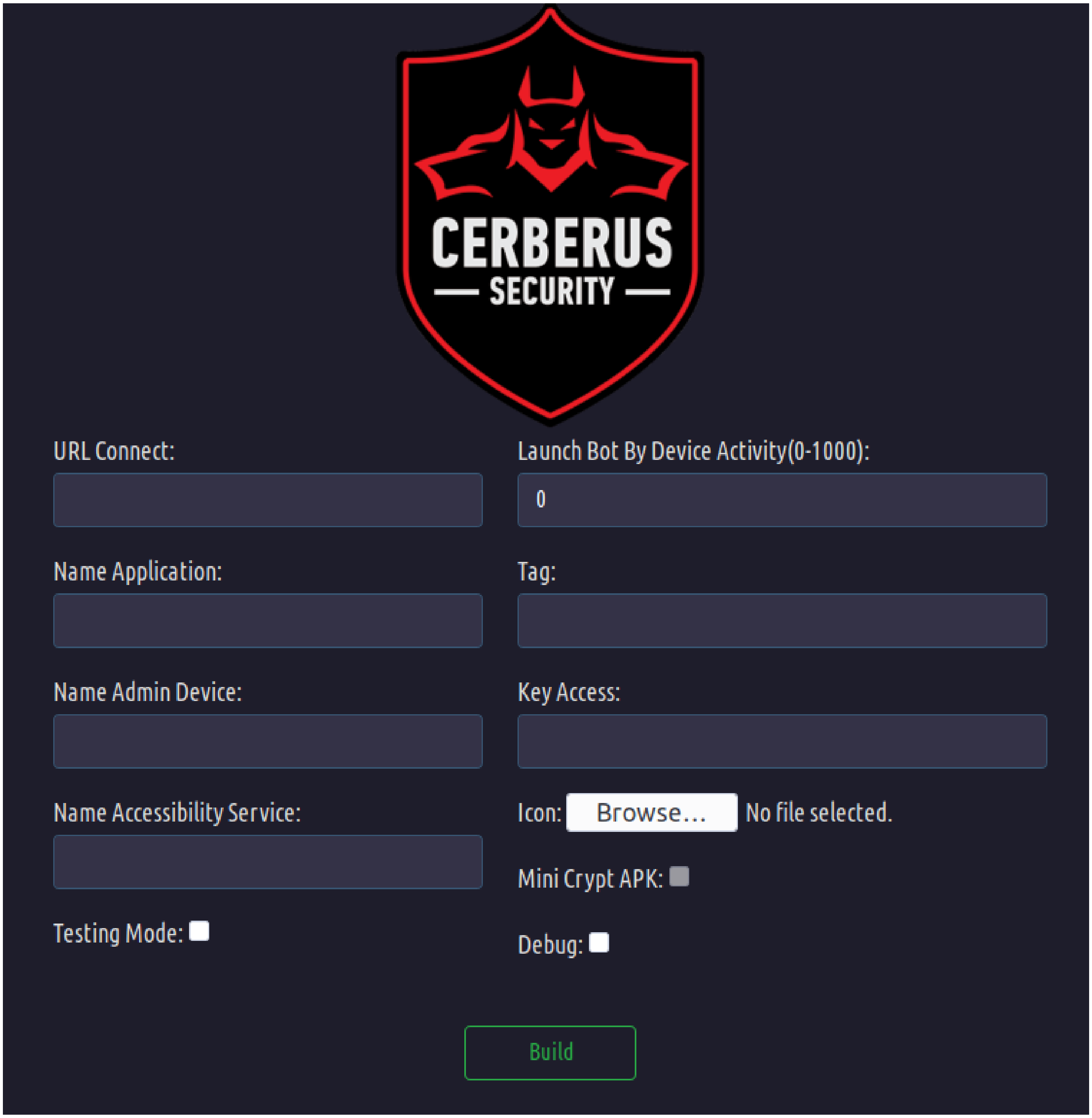
Cerberus @AndroidCerberus · Nov 28, 2019

We are making price cuts before the new year!
Hurry up to buy the Cerberus license at new prices until December 10!

3 months - $ 3,500
6 months - $ 5,500
12 months - $ 9,000
xss.is/threads/29932/...

Figure 2 – Cerberus ‘Winter Sale’

Having purchased a licence, nefarious users would gain access to the Cerberus control panel which allowed them to build an Android application package (Figure 3), in the form of an ‘APK’ file ready for distribution to victims, as well as providing them with the ability to manage their compromised devices and access any stolen data (Figure 4).



URL Connect:

Launch Bot By Device Activity(0-1000): 0

Name Application:

Tag:

Name Admin Device:

Key Access:

Name Accessibility Service:

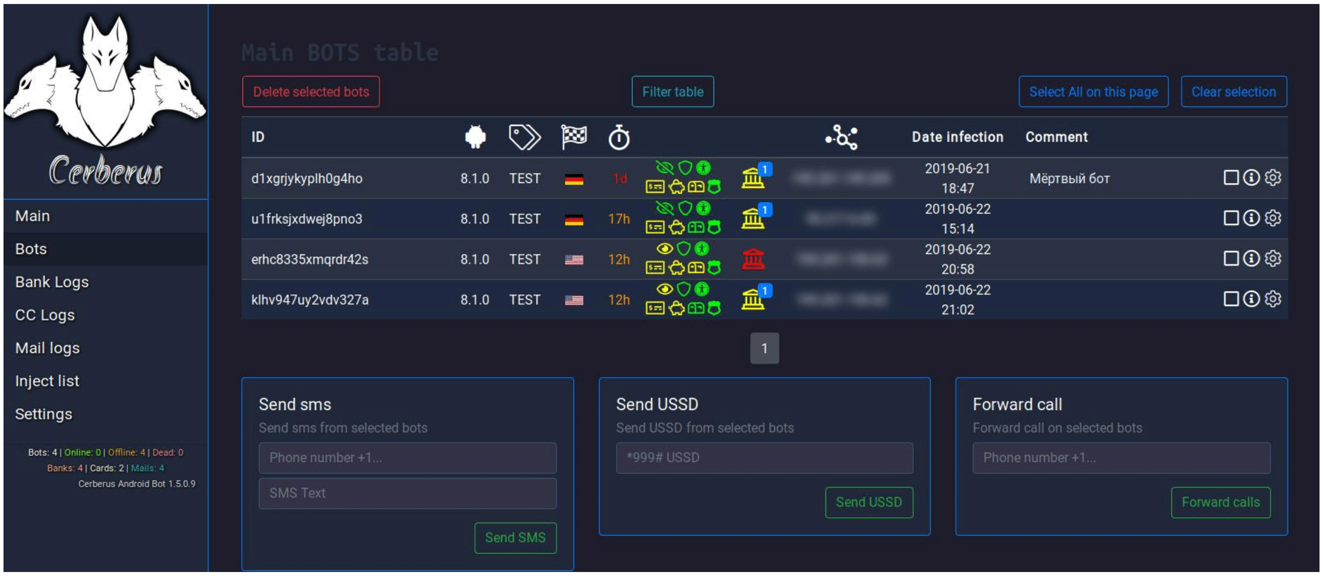
Icon: No file selected.

Mini Crypt APK: □

Testing Mode: □

Debug: □

Figure 3 – Cerberus APK builder (added to the platform in July 2019)

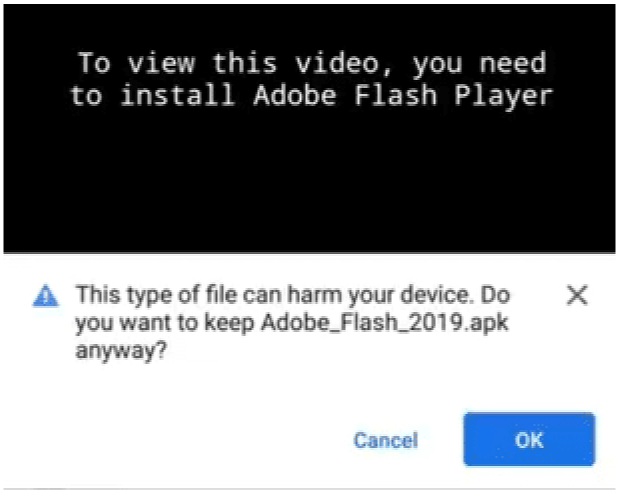


Bots: 4 | Online: 0 | Offline: 4 | Dead: 0
Banks: 4 | Cards: 2 | Mails: 4
Cerberus Android Bot 1.5.0.9

ID								Date infection	Comment	
d1xgrjykyplh0g4ho	8.1.0	TEST		1d		1	[redacted]	2019-06-21 18:47	Мёртвый бот	□
u1frksjxdwej8pno3	8.1.0	TEST		17h		1	[redacted]	2019-06-22 15:14		□
erhc8335xmqrdr42s	8.1.0	TEST		12h			[redacted]	2019-06-22 20:58		□
klhv947uy2vdv327a	8.1.0	TEST		12h		1	[redacted]	2019-06-22 21:02		□

Figure 4 – Cerberus Control Panel

Having configured and generated an APK payload file, threat actors would then need to deliver this to victims likely through the use of social engineering tactics and campaigns such as ‘fake media player’ messages shown to Android users visiting a compromised or malicious website (Figure 5) as well as fake mobile apps uploaded to various app stores and even the use of COVID-19 themes during the global pandemic.



To view this video, you need to install Adobe Flash Player

This type of file can harm your device. Do you want to keep Adobe_Flash_2019.apk anyway?

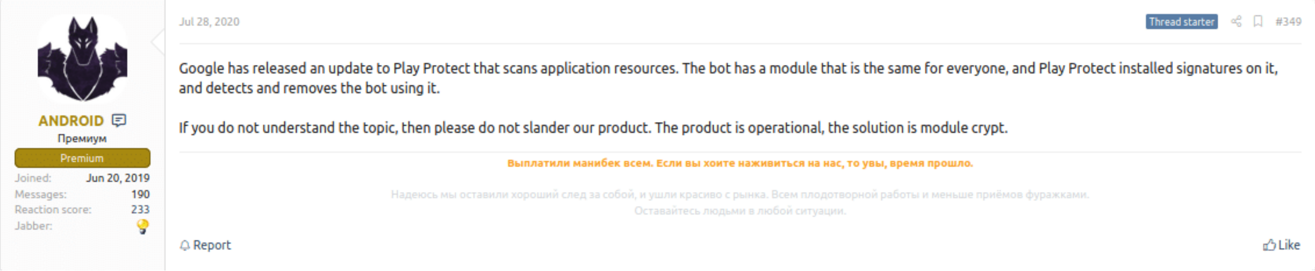
Figure 5 – Cerberus distributed via fake Adobe Flash Player (Credit: ESET Research)

Reportedly one of the most successful Android banking trojans and MaaS threats of 2019 and into 2020, Cerberus’ reign came to a somewhat abrupt end in August 2020 with the creator citing ‘internal issues’ that prevented ongoing development and undoubtedly contributed to the threat being detected and blocked by Google’s built-in antimalware protection ‘Google Play Protect’.

Attempted Sale

Whilst still in development as late as 21 July 2020, seemingly the period between 22 and 26 July 2020 saw Cerberus being detected by Google Play Protect and customers taking to the forum to complain about their ‘bots dropping off’.

In response to these complaints, ‘Android’, Cerberus’ creator or the group’s spokesperson, suggested on 28 July 2020 that the threat was still operational, albeit requiring the use of a ‘cryptor’ to prevent detection (Figure 6).



Google has released an update to Play Protect that scans application resources. The bot has a module that is the same for everyone, and Play Protect installed signatures on it, and detects and removes the bot using it.

If you do not understand the topic, then please do not slander our product. The product is operational, the solution is module crypt.

Выплатили манибек всем. Если вы хоите наживиться на нас, то увы, время прошло.

Надеюсь мы оставили хороший след за собой, и ушли красиво с рынка. Всем плодотворной работы и меньше приёмов фуражками.
Оставайтесь людьми в любой ситуации.

Figure 6 – ‘Android’ responding in English, rather than Russian, to various complaints about Cerberus on 28 July 2020

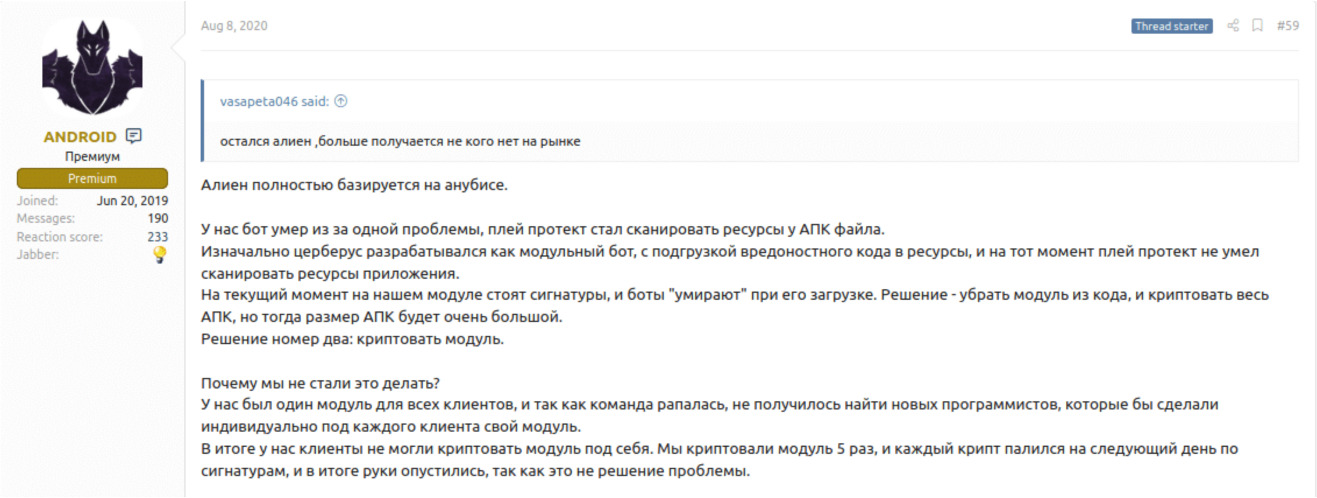
Tools known as ‘cryptors’ are often used by malware authors and utilize various encryption routines to thwart the analysis of malicious binaries as well as obfuscating or modifying their code to evade detection signatures. In this instance, it appears that the solution to Cerberus’ problems was not as simple as using a ‘cryptor’ and was promptly followed by the group ceasing development following ‘internal issues’.

In addition to the threat group reportedly disbanding, with existing Ceberus infections being in-operational due to their detection, the malware-as-a-service (MaaS) offering, including all source code, installation guides, and setup scripts along with details of current and prospective customers, was reportedly offered for auction at the end of July 2020 with a starting price of USD 50,000 and a ‘buy-it-now’ price of USD 100,000.

Appearing somewhat steeply priced, it is likely that a suitably motivated and skilled threat actor could have recouped their outlay within a year, especially given the reported USD 10,000 monthly earnings, although, given that the auction failed to find a buyer, the ‘market’ didn’t agree with this valuation or the viability of Cerberus following its detection by Google Play Protect.

Source Code Release

Following the failed auction attempt, and potentially in an attempt to restore confidence in the group, ‘Android’ posted a message to the ‘XSS[.]is’ forum on 5 August 2020 to confirm that they would be fulfilling any financial commitments to existing customers, presumably by refunding them any access payments, and that the source code would be made available to the forum’s members (Figure 7).



Joined: Jun 20, 2019
Messages: 190
Reaction score: 233
Jabber:

Aug 8, 2020

> vasapeta046 said:
>
> остался алиен ,больше получается не кого нет на рынке

Алиен полностью базируется на анубисе.

У нас бот умер из за одной проблемы, плей протект стал сканировать ресурсы у АПК файла.
Изначально церберус разрабатывался как модульный бот, с подгрузкой вредоностного кода в ресурсы, и на тот момент плей протект не умел сканировать ресурсы приложения.
На текущий момент на нашем модуле стоят сигнатуры, и боты "умирают" при его загрузке. Решение - убрать модуль из кода, и криптовать весь АПК, но тогда размер АПК будет очень большой.
Решение номер два: криптовать модуль.

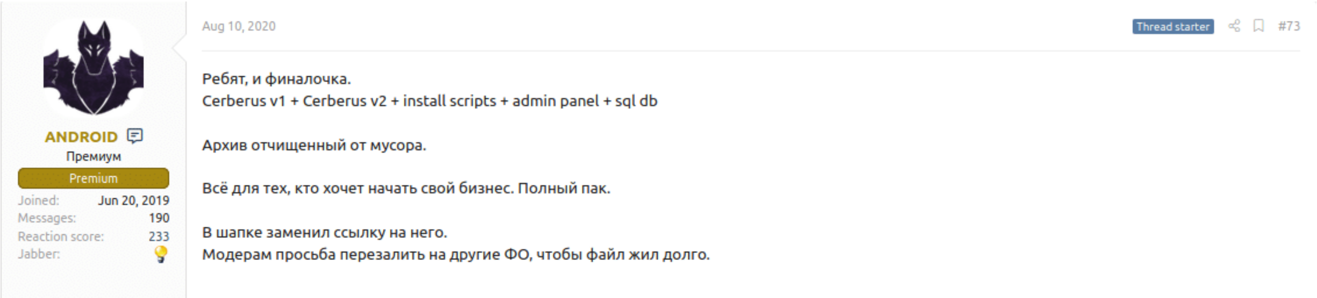
Почему мы не стали это делать?
У нас был один модуль для всех клиентов, и так как команда рапалась, не получилось найти новых программистов, которые бы сделали индивидуально под каждого клиента свой модуль.
В итоге у нас клиенты не могли криптовать модуль под себя. Мы криптовали модуль 5 раз, и каждый крипт палился на следующий день по сигнатурам, и в итоге руки опустились, так как это не решение проблемы.

Figure 7 – Forum post indicating the release of the Cerberus Source Code to members of XSS[.]is

Translation:

v2 version. Flipper.
Since our team (before that the team) ran this business cleanly, as beautifully as possible, we will finish it beautifully.
For 70% of clients, financial obligations have already been closed. The remaining ones are asked to unsubscribe in a PM or Telegram, do not forget to write your Jabber, the license key and the server IP. This is so that I can be sure that you are the owner of the license. It is also advisable to attach the APK file.
Sources to be torn apart, especially for xss[.]is
Cerberus v1 + Cerberus v2 + install scripts + admin panel + sql db

Seemingly available on various underground forums from around 7 August 2020, a subsequent post by ‘Android’ on the XSS[.]is forum on 10 August 2020 included a cleaned-up archive (Figure 8).



Joined: Jun 20, 2019
Messages: 190
Reaction score: 233
Jabber:

Aug 10, 2020

Ребят, и финалочка.
Cerberus v1 + Cerberus v2 + install scripts + admin panel + sql db

Архив отчищенный от мусора.

Всё для тех, кто хочет начать свой бизнес. Полный пак.

В шапке заменил ссылку на него.
Модерам просьба перезалить на другие ФО, чтобы файл жил долго.

Figure 8 – Cerberus source code release on XSS[.]is

Translation:

Guys, and wrap-up.

Cerberus v1 + Cerberus v2 + install scripts + admin panel + sql db

Archive cleared of garbage.

Everything for those who want to start their own business. Full pack.
In the header, I replaced the link to it.

For moderators, please re-upload to other [file sharing services] so that the file will live for a long time.

Analysis of the source code archive indicates that the directories have modification dates of 5 August 2020, confirming the archive creation of the file that aligns with the forum posts, whilst the files, excluding any open-source libraries used, have various modification dates between 31 March 2019 and July 21 2020, again consistent with what is known about Cerberus' recent development.

Note: *For reference, sample file hashes for the released Cerberus source code are provided in Appendix A.*

Included within the main archive are four main directories:

- `moduleBot2` – Java source code and assets for the Cerberus v2 Android payload including build files for use with the 'Gradle' build automation tool. Based on application icons found within the directory structure, the threat appears to mimic a 'Santander' banking app but it is understood that this would be customizable when using the 'builder' control panel.
- `panel_v2` – HTML, JavaScript and PHP source code for the server that provides the Cerberus control panel, APK payload builder and the command and control (C2) call-home 'gate.php' script. Notably, the payload builder takes parameters from the threat actor and then executes the Gradle build automation tool before allowing the payload to be downloaded. Additionally, 'cryptor' code appears within this directory that could allow payloads to thwart analysis or detection albeit, based on the Google Play Protect detection, this has been countered.
- `restapi_v2` – Seemingly allowing interactions between bots and the C2 server/control panel, the REST API directory includes PHP code and provides an insight into the status of a bot including the relatively short period of time elapsed for it to be considered 'dead' (albeit understandable given that most people will keep their mobile phone online at all times):
    - `0` – Online (Bot has been visible within the last 2 minutes);
    - `1` – Offline (Bot has been visible within the 40hrs but not last 2 minutes);
    - `2` – Dead (Bot has not been seen within the last 40hrs);

- `source_mmm` – Java source code and assets for the Cerberus v1 Android payload, again including build files for use with the ‘Gradle’ build automation tool. Furthermore, a SQL dump file is included within the archive and provides an insight into the backend database behind the Cerberus control panel. In addition to this database backup detailing the data stored on bots and compromised hosts, base64-encoded ‘injects’ are included to mimic and steal credentials or payment card data by posing as the following Android applications:
  - Connect for Hotmail & Outlook (`com.connectivityapps.hotmail`)
  - Gmail (`com.google.android.gm`)
  - Imo (`com.imo.android.imoim`)
  - Instagram (`com.instagram.android`)
  - mail.com Mail (`com.mail.mobile.android.mail`)
  - Microsoft Outlook (`com.microsoft.office.outlook`)
  - Snapchat (`com.snapchat.android`)
  - Telegram (`org.telegram.messenger`)
  - Twitter (`com.twitter.android`)
  - Uber (`com.ubercab`)
  - Viber Messenger (`com.viber.voip`)
  - WeChat (`com.tencent.mm`)
  - WhatsApp Messenger (`com.whatsapp`)
  - Yahoo Mail (`com.yahoo.mobile.client.android.mail`)

Current Capabilities

Whilst the immediate threat from Cerberus has been countered by Google Play Protect, the release of the source code provides other threat actors with the ability to analyse and understand how Cerberus’ modular capabilities were implemented, potentially allowing others to extend them or reuse the code in other Android threats.

As is to be expected of a successful Android threat, Cerberus claims to work on devices using Android 5 or later and, have gained ‘accessibility’ permissions, can automatically permit additional permissions for itself including:

- `android.permission.INTERNET` ;
- `android.permission.CALL_PHONE` ;
- `android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS` ;
- `android.permission.RECEIVE_BOOT_COMPLETED` ;
- `android.permission.READ_PHONE_STATE` ;
- `android.permission.REQUEST_DELETE_PACKAGES` ;
- `android.permission.RECEIVE_SMS` ;
- `android.permission.READ_SMS` ;
- `android.permission.SEND_SMS` ;
- `android.permission.READ_CONTACTS` ;

- `android.permission.WAKE_LOCK` ;

Given these permissions, many capabilities can be identified, such as those that are consistent with a remote access trojan gaining access to, and control over, the device:

- Screenshot and audio recording;
- Keylogging from within applications;
- Access and exfiltrate contacts;
- Device location tracking;
- Application download, execution and removal;
- Device lock;
- Mute all device sound and disable vibrate alerts;

Additionally, specific banking trojan capabilities provide the means to gather credentials and payment card data as well as thwarting additional security measures such as one-time passwords, multi-factor authentication and voice calls:

- Access, send, receive and delete SMS (ideal for capturing one-time passwords);
- Call forwarding (potentially allowing the interception of voice calls);
- Credential and payment card data theft through application injections;
- Local installation and automatic (timed) enable of injections to allow operation with limited network coverage;
- Theft of multi-factor authentication codes from Google Authenticator;

In an attempt to evade security controls and thwart analysis, Cerberus implemented anti-emulator code to ensure that it was only executed on a valid physical device, attempted to disable Google Play Protect, albeit until its detection, and provided a self-destruct mechanism to remove traces of the bot to prevent post-incident analysis.

Finally, command and control (C2) traffic is RC4 encrypted and base64-encoded using a random key. Subsequently, 'call home' communications include useful data about the device which is viewable within the control panel:

- Android operating system version;
- Battery status;
- Device manufacturer/model;
- IP address;
- Network operator;
- Telephone number;
- System locale (Country and language);
- Screen status (Locked or Unlocked);
- Google Play Protect status;
- SMS intercept status;
- Availability of bank, card and email credentials/data;

- Infection date and bot up-time;
- Telephone activity, used to determine if it is an emulator;

Features: hide SMS, lock device, mute sound, keylogger, injection

Injections

Cerberus makes use of ‘injections’ to target legitimate applications, including those related to banking, email, messaging, retail and social media, with pages that mimic the targeted application interface and prompt for credentials and/or payment card details from the victim (Figure 9).

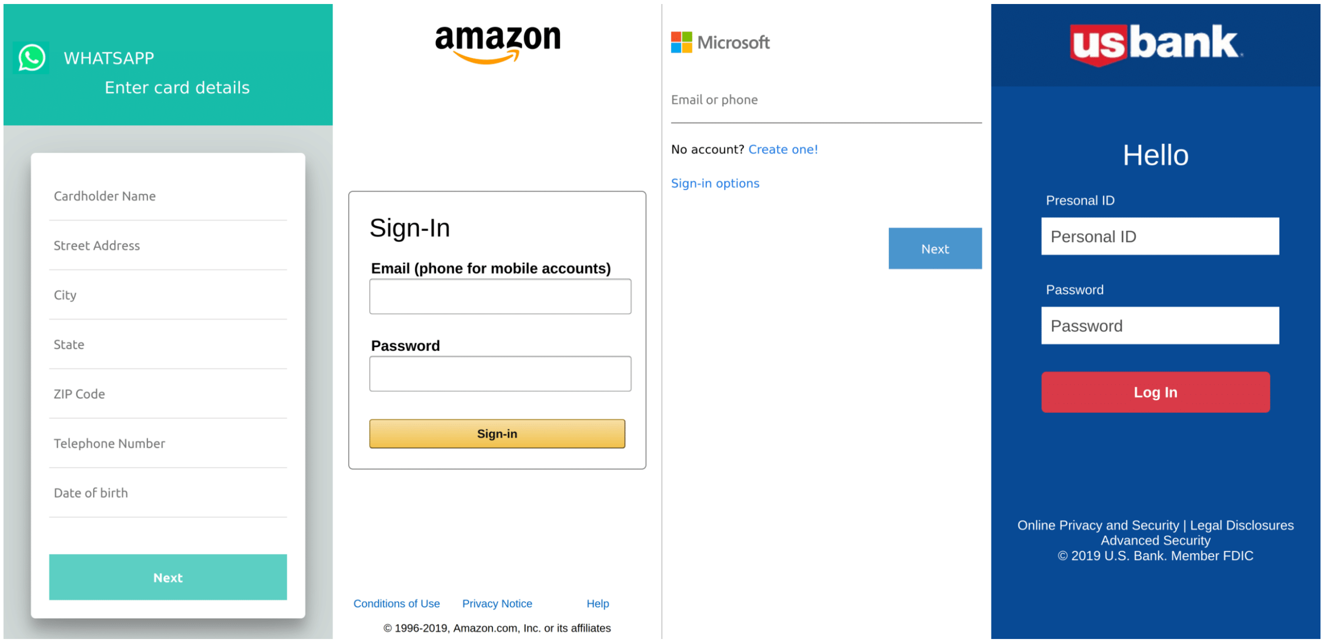
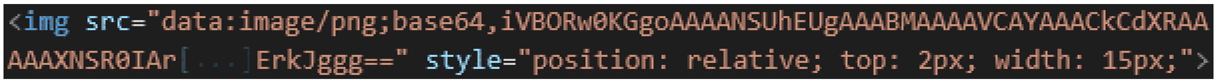


Figure 9 – Example ‘injects’ mimicking legitimate application interfaces

These HTML-based injects are provided as a single file asset, allowing them to be easily stored within the command and control (C2) database and distributed to victim devices, integrating cascading style sheets (CSS) to ensure the layout is consistent with the targeted application as well as embedding base64-encoded images (Figure 10).

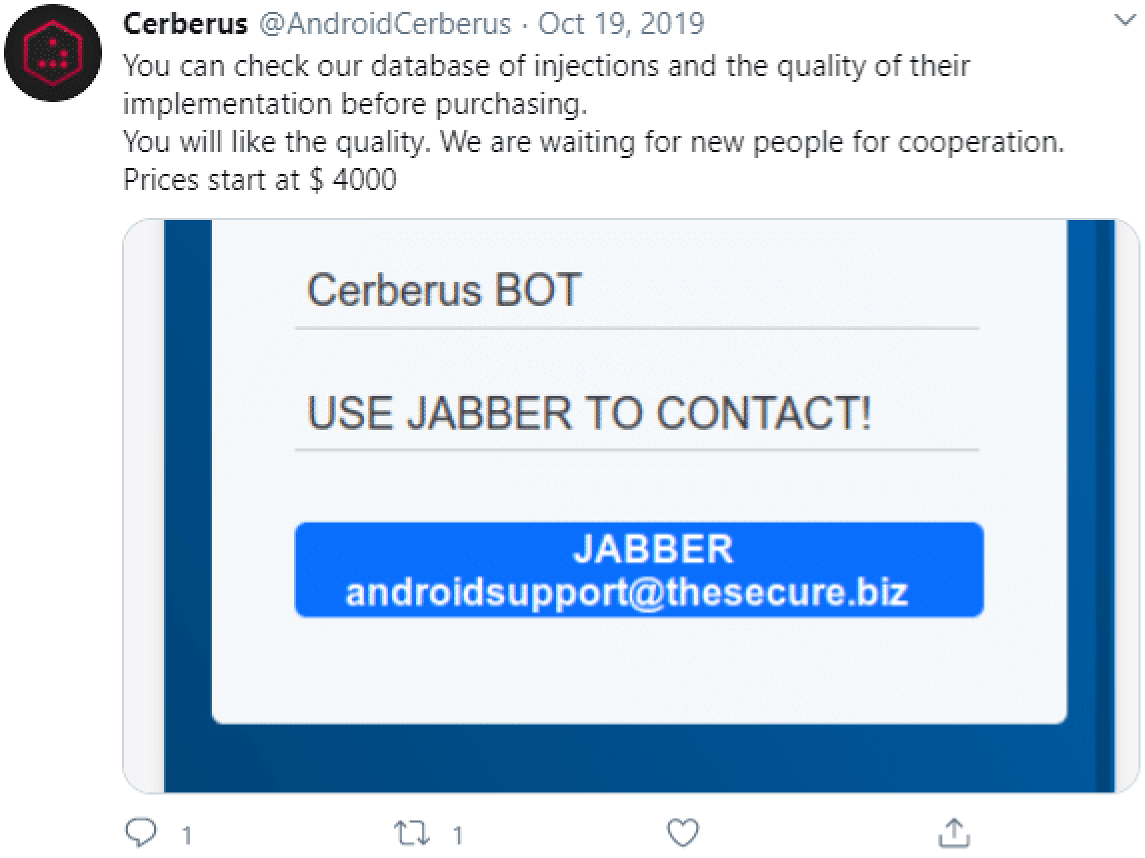


```
<img src="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAABMAAAAVCAYAAACkCdXRAA
AAAXNSR0IAr[...]ErkJggg==" style="position: relative; top: 2px; width: 15px;">
```

Figure 10 – Example embedded base64-encoded PNG image within the inject HTML file

Once deployed, a victim would be presented with the inject when attempting to access a targeted application and, assuming they fall for the ruse, the data entered is inserted into a JSON data structure ready for exfiltration by Cerberus to the C2 infrastructure.

Seemingly a ‘starter kit’ was offered by Cerberus with a handful of injections to target Italy, France, Turkey and the United States, whilst additional injections could be purchased (Figure 11).



Cerberus @AndroidCerberus · Oct 19, 2019

You can check our database of injections and the quality of their implementation before purchasing.
You will like the quality. We are waiting for new people for cooperation.
Prices start at $ 4000

Cerberus BOT

USE JABBER TO CONTACT!

JABBER
androidsupport@thesecure.biz

Figure 11 – Cerberus ‘Tweet’ indicating the sale of injects

Notably, in addition to base64-encoded injects embedded within the SQL dump file distributed with the Cerberus control panel source code, archives of this recent release distributed on underground forums include over 200 additional inject files potentially including some that would have previously been charged for.

Note: *For reference, a full list of the injects distributed with the Cerberus source code are provided in Appendix B.*

Given that these inject files mimic many current mobile applications, the release of this large set could allow other malware authors to incorporate them into their own mobile threats as well as being of use to any threat actor that can make use of, or further develop, the Cerberus source code.

Potential Future Developments

Increased Targeting

As is common with cybercrime threats originating from Russia or countries within the Commonwealth of Independent States (CIS), threat actors will only target victims in other countries as confirmed by a string variable within Cerberus' source code containing a safe list of country codes:

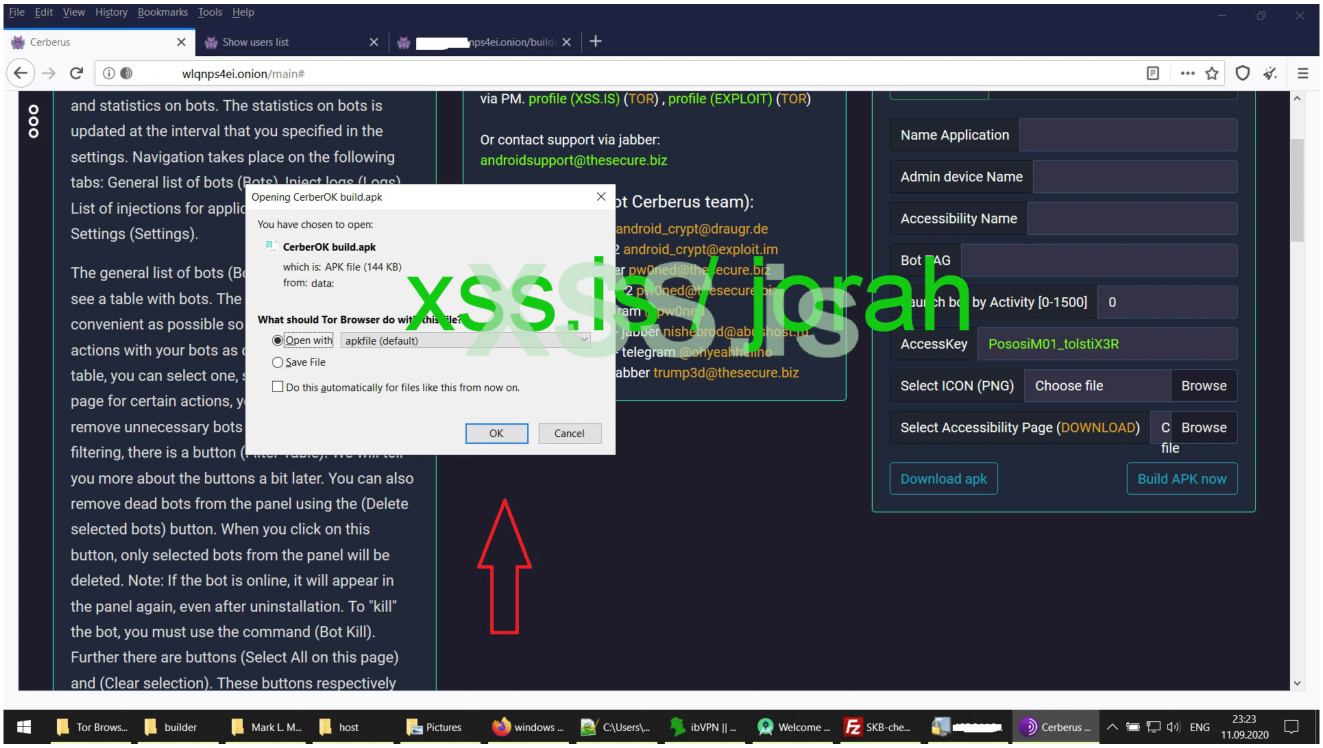
```
public String strCIS = "[ua][ru][by][tj][uz][tm][az][am][kz][kg][md]";
```

Since the public release of Cerberus' source code, other seemingly less-patriotic threat actors have removed or modified this restriction and there is now reportedly an increase in victims within Russia and CIS countries.

Aside than this shift in targeting, no other region has been identified as suffering from increased attacks although, with time, other threat actors may seek to leverage their access to the source code and potentially launch attacks in regions where Android devices are prevalent whilst less likely to be protected by current versions of Google Play Protect.

Variants

In addition to threat actors taking the Cerberus source code 'as-is' and attempting to launch their own campaigns, especially given that an 'enterprising' user on the XSS[.]is forum is offering an installation service for just USD 300 (Figure 12), others may seek to build upon the existing code or create their own variants to resolve the issues that caused Google Play Protect to detect the threat.



and statistics on bots. The statistics on bots is
updated at the interval that you specified in the
settings. Navigation takes place on the following
tabs: General list of bots (Bots), Inject logs (Logs)
List of injections for applic
Settings (Settings).

The general list of bots (Bo
see a table with bots. The
convenient as possible so
actions with your bots as c
table, you can select one, s
page for certain actions, y
remove unnecessary bots
filtering, there is a button (
you more about the buttons a bit later. You can also
remove dead bots from the panel using the (Delete
selected bots) button. When you click on this
button, only selected bots from the panel will be
deleted. Note: If the bot is online, it will appear in
the panel again, even after uninstallation. To "kill"
the bot, you must use the command (Bot Kill).
Further there are buttons (Select All on this page)
and (Clear selection). These buttons respectively

via PM. profile (XSS.IS) (TOR) , profile (EXPLOIT) (TOR)

Or contact support via jabber:
androidsupport@thesecure.biz

ot Cerberus team):
android_crypt@draugr.de
2 android_crypt@exploit.im
er pw0ned@thesecure.biz
2 pw0ned@thesecure.biz
ram @pw0ne
- jabber nishebrod@abushost.ru
- telegram @ohyeahhellno
abber trump3d@thesecure.biz

Opening CerberOK build.apk

You have chosen to open:

CerberOK build.apk
which is: APK file (144 KB)
from: data:

What should Tor Browser do with this file?

● Open with apkfile (default)
○ Save File
□ Do this automatically for files like this from now on.

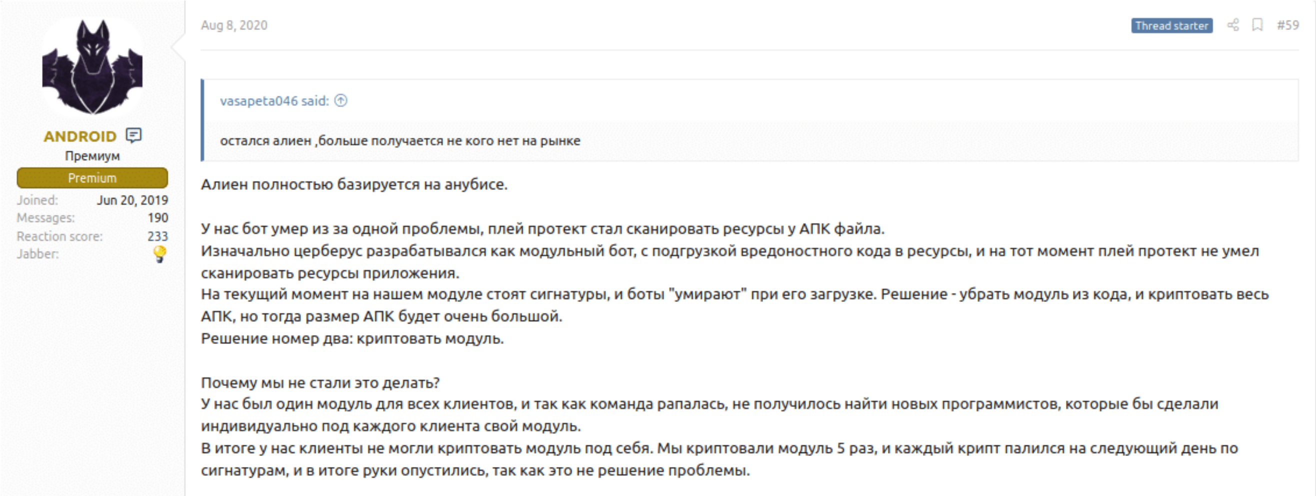
OK Cancel

Name Application
Admin device Name
Accessibility Name
Bot TAG
Launch bot by Activity [0-1500] 0
AccessKey PososiM01_tolstiX3R
Select ICON (PNG) Choose file Browse
Select Accessibility Page (DOWNLOAD) Choose file Browse
Download apk
Build APK now

Figure 12 – XSS[.]is forum member offering proof of their Cerberus install service

One such example that has been reported as a variant of Cerberus is a threat dubbed ‘Alien’ although, both the creators of Alien and Cerberus have denied any link between the two.

Providing any would-be successor with the necessary information to resolve Cerberus’ issues, two suggestions are given to counter Google Play Protect’s ability to scan application resources (Figure 13).



Aug 8, 2020

> vasapeta046 said:
>
> остался алиен ,больше получается не кого нет на рынке

Алиен полностью базируется на анубисе.

У нас бот умер из за одной проблемы, плей протект стал сканировать ресурсы у АПК файла.
Изначально церберус разрабатывался как модульный бот, с подгрузкой вредоностного кода в ресурсы, и на тот момент плей протект не умел сканировать ресурсы приложения.
На текущий момент на нашем модуле стоят сигнатуры, и боты "умирают" при его загрузке. Решение - убрать модуль из кода, и криптовать весь АПК, но тогда размер АПК будет очень большой.
Решение номер два: криптовать модуль.

Почему мы не стали это делать?
У нас был один модуль для всех клиентов, и так как команда рапалась, не получилось найти новых программистов, которые бы сделали индивидуально под каждого клиента свой модуль.
В итоге у нас клиенты не могли криптовать модуль под себя. Мы криптовали модуль 5 раз, и каждый крипт палился на следующий день по сигнатурам, и в итоге руки опустились, так как это не решение проблемы.

Figure 13 – Denial of link to ‘Alien’ and Cerberus ‘solution’ proposals
Translation:
Alien is based entirely on Anubis.
Our bot died due to one problem, the play-protection started scanning the resources of the APK file.
Initially, Cerberus was developed as a modular bot, loading malicious code into resources, and at that time Play Protect was unable to scan application resources.
At the moment, our module has signatures, and bots “die” when it is loaded. The solution is to remove the module from the code and encrypt the entire APK, but then the size of the APK will be very large.
Solution number two: encrypt the module.
Why didn’t we do it?
We had one module for all clients, and since the team was crumbling, it was not possible to find new programmers who would make their own module for each client individually.
As a result, our clients could not encrypt the module for themselves. We encrypted the module 5 times, and each crypt fell the next day according to the signatures, and in the end our hands dropped, since this is not a solution to the problem.

Whilst it is likely only a matter of time before a suitably skilled nefarious developer resolves the issues with Cerberus, the release of the source code will undoubtedly assist the Google Play Protect team in creating countermeasures. That being said, organizations should still encourage users to, and individuals should, be cautious whenever prompted to install Android packages (APK) from unverified sources, be that a browser pop-up, an email or from a third-party app marketplace.

Appendix A – Samples

The following SHA-256 file hashes relate to the leaked files, as observed on multiple underground forums, and may prove beneficial to security professionals wishing to perform their own analysis of the threat:

- Initial source code release `cerberus_full_package.7z`
  `2ba17fabce13866b6f161250f00d85e14fefc6334dc1bdd881bb71ba41a69d80`
- ‘Cleaned-up’ source code release `CERBERUS_V2.zip`
  `733fc478acd6ef668f88131f505921fddc88e9a207e5ee304b37babf0b8a553d`
- Injections collection `injects.zip`
  `856ea6fd89f431274335614e91fdd83a99aaa3243395a28d7e55307a04090923`
- Bundle containing the above, released on ‘Alphazine[.]ru’ `cerberus.zip`
  `beabdc7eedea45771c11e2319f810035fdbf67e725b593a80ef54438ee3731f5`

Given the current status of Cerberus, indicators of compromise (IOC) related to past Cerberus threats are somewhat redundant although the command and control (C2) Tor hidden service still appears to be accessible via `cerberesfgqzqou7.onion` (Figure 14).

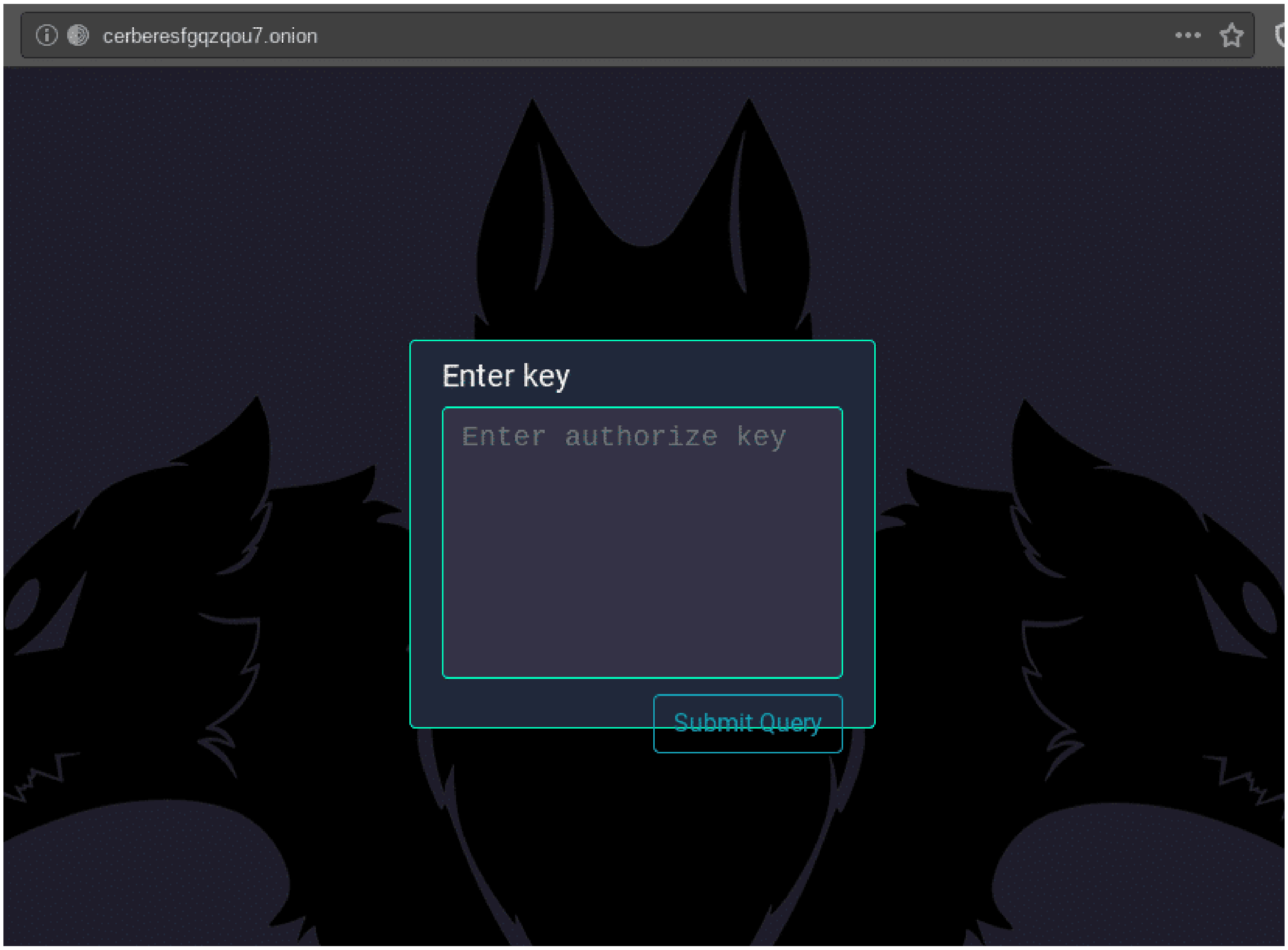


Figure 14 – Cerberus control panel Tor hidden service

Additionally, the following HTTP command and control (C2) communication strings were observed within the source code and may appear in derivative works:

- `action=getinj&data=` ;
- `action=injcheck&data=` ;
- `action=botcheck&data=` ;
- `||no||` ;
- `action=registration&data=` ;
- `action=sendInjectLogs&data=` ;
- `action=sendSmsLogs&data=` ;
- `action=timeInject&data=` ;public String str_http_19 = “action=sendKeylogger&data=”; public String str_http_20 = “action=getModule&data=”; public String str_http_21 = “action=checkAP&data=”;
- `action=sendKeylogger&data=` ;
- `action=getModule&data=` ;
- `action=checkAP&data=` ;

Appendix B – Injections

Injection files have been provided alongside the Cerberus source code and target the following legitimate Android applications:

- ABANCA Empresas `com.abanca.bancaempresas`
- ABANCA Banca Móvil `es.caixagalicia.activamovil`
- ABN AMRO Mobiel Bankieren `com.abnamro.nl.mobile.payments`
- Akbank `com.akbank.android.apps.akbank_direkt`
- Allegro `pl.allegro`
- Amazon Shopping `com.amazon.mShop.android.shopping`
- ASB Mobile Banking `nz.co.asb.asbmobile`
- Banca Digital Liberbank `es.liberbank.cajasturapp`
- Banca Móvil Laboral Kutxa `com.tecnocom.cajalaboral`
- Banca MPS `copergmps.rt.pf.android.sp.bmps`
- Banca Transilvania `ro.btrl.mobile`
- Banco Caixa Geral España `es.caixageral.caixageralapp`
- Banco Itaú Empresas `com.itau.empresas`
- Banco Sabadell `net.inverline.bancosabadell.officelocator.android`
- Bank Austria MobileBanking `com.bankaustria.android.olb`
- Bank Hapoalim (בנק הפועלים) `com.ideomobile.hapoalim`
- Bank Millennium `wit.android.bcpBankingApp.millenniumPL`
- Bank Millennium for Companies `pl.millennium.corpApp`
- Bank of America Mobile Banking `com.infonow.bofa`
- Bank of Melbourne Mobile Banking `org.bom.bank`
- Bankia `es.cm.android`

- Bankinter Móvil `com.bankinter.launcher`
- BankSA Mobile Banking `org.banksa.bank`
- Banque `com.caisseepargne.android.mobilebanking`
- Banque Populaire `fr.banquepopulaire.cyberplus`
- Banque pour tablettes Android `com.caisse.epargne.android.tablette`
- Barclays `com.barclays.android.barclaysmobilebanking`
- Barclays Kenya `com.barclays.ke.mobile.android.ui`
- BBVA Net Cash `com.bbva.netcash`
- BBVA Spain `com.bbva.bbvacontigo`
- BEA (東東亞亞銀銀行行) `com.mtel.androidbea`
- Bendigo Bank `com.bendigobank.mobile`
- BHIM UPI, Money Transfer, Recharge & Bill Payment `com.mobikwik_new`
- Bi en Línea `gt.com.bi.bienlinea`
- Bill Payment & Recharge,Wallet `com.oxigen.oxigenwallet`
- Binance `com.binance.dev`
- bitbank `cc.bitbank.bitbank`
- Bitcoin Wallet Coincheck `jp.coincheck.android`
- Blockchain Wallet `piuk.blockchain.android`
- BMO Mobile Banking `com.bmo.mobile`
- BNL `it.bnl.apps.banking`
- BNP Paribas GOMobile `com.finanteq.finance.bgz`
- BOCHK `com.bochk.com`
- BOQ Mobile `com.bankofqueensland.boq`
- Boursorama Banque `com.boursorama.android.clients`
- BPI APP `pt.bancobpi.mobile.fiabilizacao`
- BPS Mobilnie `pl.bps.bankowoscmobilna`
- BusinessPro Lite `pl.bph`
- CA24 Mobile `com.finanteq.finance.ca`
- CaixaBank `es.lacaixa.mobile.android.newwapicon`
- Caixadirecta `cgd.pt.caixadirectaparticulares`
- Cajalnet `es.ceca.cajalnet`
- Cajasur `com.cajasur.android`
- Capital One® Mobile `com.konylabs.capitalone`
- Carige Mobile `it.carige`
- Carrefour Finance `be.fimaser.smartphone`
- Ceneo `pl.ceneo`
- CEPTETEB `com.teb`
- Chase Mobile `com.chase.sig.android`
- CIBC Mobile Banking `com.cibc.android.mobi`
- CIC `com.cic_prod.bad`
- Citi Handlowy `com.konylabs.cbplpat`
- CMSO my bank `com.arkea.android.application.cmso2`

- Coinbase Wallet — Crypto Wallet & DApp Browser `org.toshi`
- comdirect mobile App `de.comdirect.android`
- CommBank `com.commbank.netbank`
- Commerzbank Banking `de.commerzbanking.mobil`
- Connect for Hotmail & Outlook `com.connectivityapps.hotmail`
- Consorsbank `de.consorsbank`
- Credem `com.CredemMobile`
- Crédit du Nord pour Mobile `com.ocito.cdn.activity.creditdunord`
- Crédit Mutuel `com.cm_prod.bad`
- Crédit Mutuel de Bretagne `com.arkea.android.application.cmb`
- ČSOB Smartbanking `cz.csob.smartbanking`
- CUA Mobile Banking `au.com.cua.mb`
- DB Pay `com.db.pbc.DBPay`
- Deutsche Bank Mobile `com.db.pwcc.dbmobile`
- Discount Bank `com.ideomobile.discount`
- Discover Mobile `com.discoverfinancial.mobile`
- DKB-Banking `de.dkb.portalapp`
- Empik `com.empik.empikapp`
- Empik Foto `com.empik.empikfoto`
- Enpara.com Cep Şubesi `finansbank.enpara`
- eurobank mobile 2.0 `pl.eurobank2`
- EVO Banco móvil `es.evobanco.bancamovil`
- Fifth Third Mobile Banking `com.clairmail.fth`
- Fortuneo, mes comptes banque & bourse en ligne `com.fortuneo.android`
- Garanti BBVA Mobile `com.garanti.cepsubesi`
- Getin Mobile `com.getingroup.mobilebanking`
- Gmail `com.google.android.gm`
- GMO Wallet `com.gmowallet.mobilewallet`
- Grupo Cajamar `com.grupocajamar.wefferent`
- Halifax Mobile Banking `com.grppl.android.shell.halifax`
- Halkbank Mobil `com.tmobtech.halkbank`
- HSBC Mobile Banking `com.htsu.hsbcpersonalbanking`
- HVB Mobile Banking `eu.unicreditgroup.hvbapptan`
- Ibercaja `es.ibercaja.ibercajaapp`
- iBiznes24 mobile `pl.bzwbk.ibiznes24`
- iBOSStoken `hr.asseco.android.mtoken.bos`
- IDBI Bank GO Mobile+ `com.snapwork.IDBI`
- Idea Bank PL `pl.ideabank.mobilebanking`
- IKO `pl.pkobp.iko`
- Imagin `com.imaginbank.app`
- imo free video calls and chat `com.imo.android.imoim`
- iMobile by ICICI Bank `com.csam.icici.bank.imobile`

- ING Banking to go `de.ingdiba.bankingapp`
- ING Business `com.comarch.security.mobilebanking`
- ING España `www.ingdirect.nativeframe`
- ING Italia `it.ingdirect.app`
- Instagram `com.instagram.android`
- Intesa Sanpaolo Mobile `com.latuabancaperandroid_2`
- Intesa Sanpaolo Mobile `com.latuabancaperandroid`
- iPKO biznes `pl.pkobp.ipkobiznes`
- İşCep `com.pozitron.iscep`
- Kraken Pro `com.kraken.trade`
- Kutxabank `com.kutxabank.android`
- Kuveyt Türk `com.kuveytturk.mobil`
- L’Appli Société Générale `mobi.societegenerale.mobile.lappli`
- La Mia Banca `com.db.pbc.miabanca`
- La Poste `fr.laposte.lapostemobile`
- Leumi (לאומי) `com.leumi.leumiwallet`
- Liquid by Quoine `com.quoine.quoinex.light`
- Lloyds Bank Mobile Banking `com.grppl.android.shell.CMBlloydsTSB73`
- Ma Banque `fr.creditagricole.androidapp`
- mail.com mail `com.mail.mobile.android.mail`
- mBank PL `pl.mbank`
- Mes Comptes `fr.lcl.android.customerarea`
- Mes Comptes BNP Paribas `net.bnpparibas.mescomptes`
- Mi Banco db `com.db.pbc.mibanco`
- Mi Banco Mobile `com.popular.android.mibanco`
- Microsoft Outlook `com.microsoft.office.outlook`
- Mizrahi Bank (מזרחי טפחות) `com.MizrahiTefahot.nh`
- Mobile Banking UniCredit `com.unicredit`
- Mobile BiznesPl@net `com.comarch.mobile.banking.bgzbnpparibas.biznes`
- Mobilni Banka `eu.inmite.prj.kb.mobilbank`
- Mobilny Portfel `pl.raiffeisen.nfc`
- Mój Orange `pl.orange.mojeorange`
- Moje ING mobile `pl.ing.mojeing`
- myAT&T `com.att.myWireless`
- N26 Mobile Banking `de.number26.android`
- NAB Mobile Banking `au.com.nab.mobile`
- NBapp Spain `com.indra.itecban.mobile.novobanco`
- Nest Bank nowy `pl.nestbank.nestbank`
- NETELLER `com.moneybookers.skrillpayments.neteller`
- norisbank App `com.db.mm.norisbank`
- Oney France `fr.oney.mobile.mescomptes`
- Openbank `es.openbank.mobile`

- Papara `com.mobillium.papara`
- PayPal Mobile Cash `com.paypal.android.p2pmobile`
- Pekao24Makler `eu.eleader.mobilebanking.pekao`
- PekaoBiznes24 `eu.eleader.mobilebanking.pekao.firm`
- PeoPay `softax.pekao.powerpay`
- People’s Choice Credit Union `com.fusion.ATMLocator`
- Pibank `es.pibank.customers`
- plusbank24 `eu.eleader.mobilebanking.invest`
- Pocket Bank `ma.gbp.pocketbank`
- Postbank Finanzassistent `de.postbank.finanzassistent`
- Postepay `posteitaliane.posteapp.apppostepay`
- QNB Finansbank Mobile Banking `com.finansbank.mobile.cepsube`
- Raiffeisen ELBA `com.isis_papyrus.raiffeisen_pay_eyewdg`
- Raiffeisen Smart Mobile `com.advantage.RaiffeisenBank`
- Rakuten Bank (楽楽天天銀銀行行) `jp.co.rakuten_bank.rakutenbank`
- RBC Mobile `com.rbc.mobile.android`
- Report `com.cajasiete.android.cajasietereport`
- Rossmann PL `pl.com.rossmann.centauros`
- ruralvía `com.rsi`
- Santander `es.bancosantander.apps`
- Santander Banking `de.santander.presentation`
- Santander Empresas `es.bancosantander.empresas`
- Santander mobile `pl.bzwbk.bzwbk24`
- ScotiaMóvil `net.garagecoders.e_llavescotiainfo`
- SCRIGNOapp `it.popso.SCRIGNOapp`
- SecureApp netbank `de.adesso_mobile.secureapp.netbank`
- ŞEKER MOBİL ŞUBE `tr.com.sekerbilisim.mbank`
- Skrill `com.moneybookers.skrillpayments`
- Smart Mobile Banking `it.gruppobper.ams.android.bper`
- Snapchat `com.snapchat.android`
- Sparkasse Ihre mobile Filiale `com.starfinanz.smob.android.sfinanzstatus`
- St.George Mobile Banking `org.stgeorge.bank`
- Sumishin SBI Net Bank (住住信信SBIネネッットト銀銀行行) `jp.co.netbk`
- Suncorp Bank `au.com.suncorp.SuncorpBank`
- SunTrust Mobile App `com.suntrust.mobilebanking`
- TARGOBANK Mobile Banking `com.targo_prod.bad`
- Telegram `org.telegram.messenger`
- The International Bank (הבנק הבינלאומי) `com.fibi.nativeapp`
- Touch 24 Banking BCR `at.spardat.bcrmobile`
- Triodos Bank `com.indra.itecban.triodosbank.mobile.banking`
- Twitter `com.twitter.android`
- U.S. Bank `com.usbank.mobilebanking`

- Uber `com.ubercab`
- UBI Banca `it.nogood.container`
- UnicajaMovil `es.univia.unicajamovil`
- Union Bank (בנק אגוד) `com.unionBank.app`
- Union Bank Mobile Banking `com.unionbank.ecommerce.mobile.android`
- USAA Mobile `com.usaa.mobile.android.usaa`
- Usługi Bankowe `alior.bankingapp.android`
- VakıfBank Mobil Bankacılık `com.vakifbank.mobile`
- Viber Messenger `com.viber.voip`
- Volksbank house banking `at.volksbank.volksbankmobile`
- VR Banking Classic `de.fiducia.smartphone.android.banking.vr`
- WeChat `com.tencent.mm`
- Wells Fargo Mobile `com.wf.wellsfargomobile`
- Western Union ES `com.westernunion.moneytransferr3app.es`
- WhatsApp Messenger `com.whatsapp`
- Yahav Bank (בנק יהב) `il.co.yahav.mobbanking`
- Yahoo Mail `com.yahoo.mobile.client.android.mail`
- Yapı Kredi Mobile `com.ykb.android`
- Yono Lite SBI `com.sbi.SBIFreedomPlus`
- YouApp `com.lynxspa.bancopopolare`
- Ziraat Mobile `com.ziraat.ziraatmobil`