BlackRock - the Trojan that wanted to get them all

threatfabric.com/blogs/blackrock_the_trojan_that_wanted_to_get_them_all.html

July 2020

Intro

Around May 2020 ThreatFabric analysts have uncovered a new strain of banking malware dubbed BlackRock that looked pretty familiar. After investigation, it became clear that this newcomer is derived from the code of the Xerxes banking malware, which itself is a strain of the LokiBot Android banking Trojan. The source code of the Xerxes malware was made public by its author around May 2019, which means that it is accessible to any threat actor.

When source code of malware is leaked or made publicly accessible it is pretty common to see the threat landscape being supplemented with new malware variants or families based on the said code. We have observed similar events in the past, as for example the infamous Bankbot Trojan code made available by its author, leading to new Trojans like CometBot, Razdel and Anubis. When Anubis itself was leaked the actor(s) behind the Ginp Trojan reused small portions of its code.

However, when Xerxes' source code was leaked, no new malware based on, or using portions of, such code was observed. BlackRock seems to be the only Android banking Trojan based on the source code of the Trojan at the moment.

Although LokiBot has been considered dead and inactive for a while, we have observed attempts from some actors to get the Trojan working several times in the last years. Looking at the number of samples built for each of those campaigns and the duration of those, the actors didn't seem to have been very successful. Therefore, we believe that those campaigns were probably driven by new actors trying out the publicly available source code. BlackRock campaigns - on the other hand - are not alike, not only did the Trojan undergo changes in its code, but also comes with an increased target list (containing many non-financial apps) and have been ongoing for a longer period.

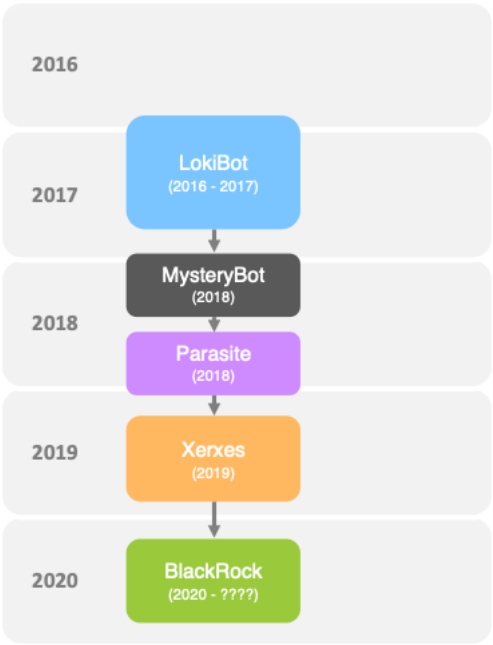
Technical aspects aside, one of the interesting differentiators of BlackRock is its target list; it contains an important number of social, networking, communication and dating applications. So far, many of those applications haven't been observed in target lists for other existing banking Trojans. It therefore seems that the actors behind BlackRock are trying to abuse the grow in online socializing that increased rapidly in the last months due to the pandemic situation.

The LokiBot malware family

As BlackRock is based on the Xerxes banking Trojan, it is part of the LokiBot descendance which has several variants, as shown hereafter.

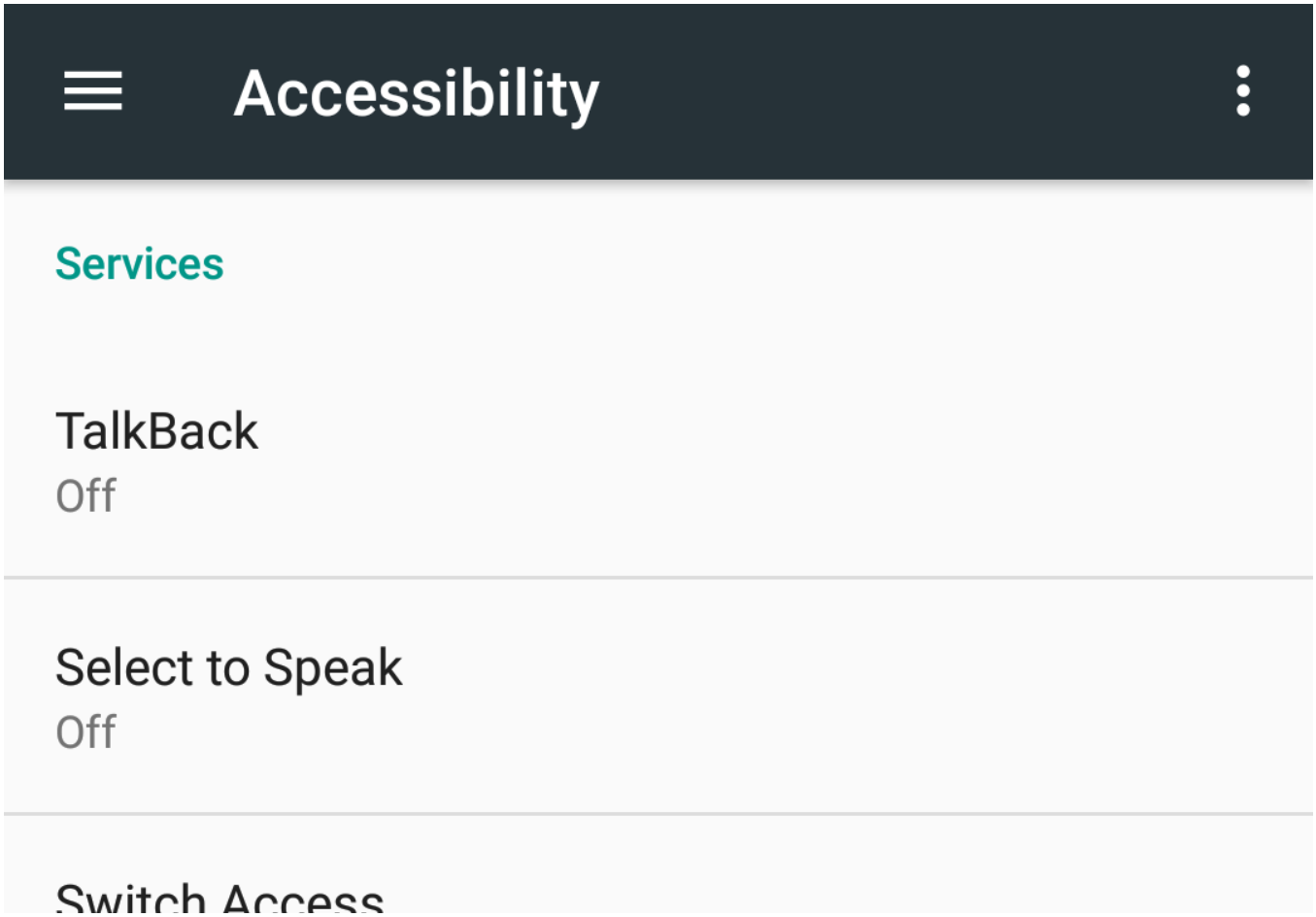
LokiBot itself was first observed between end 2016 and beginning 2017 as rented malware. Sometime after the author of the Trojan got banned from underground forums, the source code of the Trojan was leaked. During first half of 2018 MysteryBot was observed to be active. Although it was based on LokiBot it contained upgrades in order to work properly on newer Android versions and used new techniques to steal personal information. In the second half of 2018, Parasite appeared on the threat landscape as direct successor of MysteryBot. It was

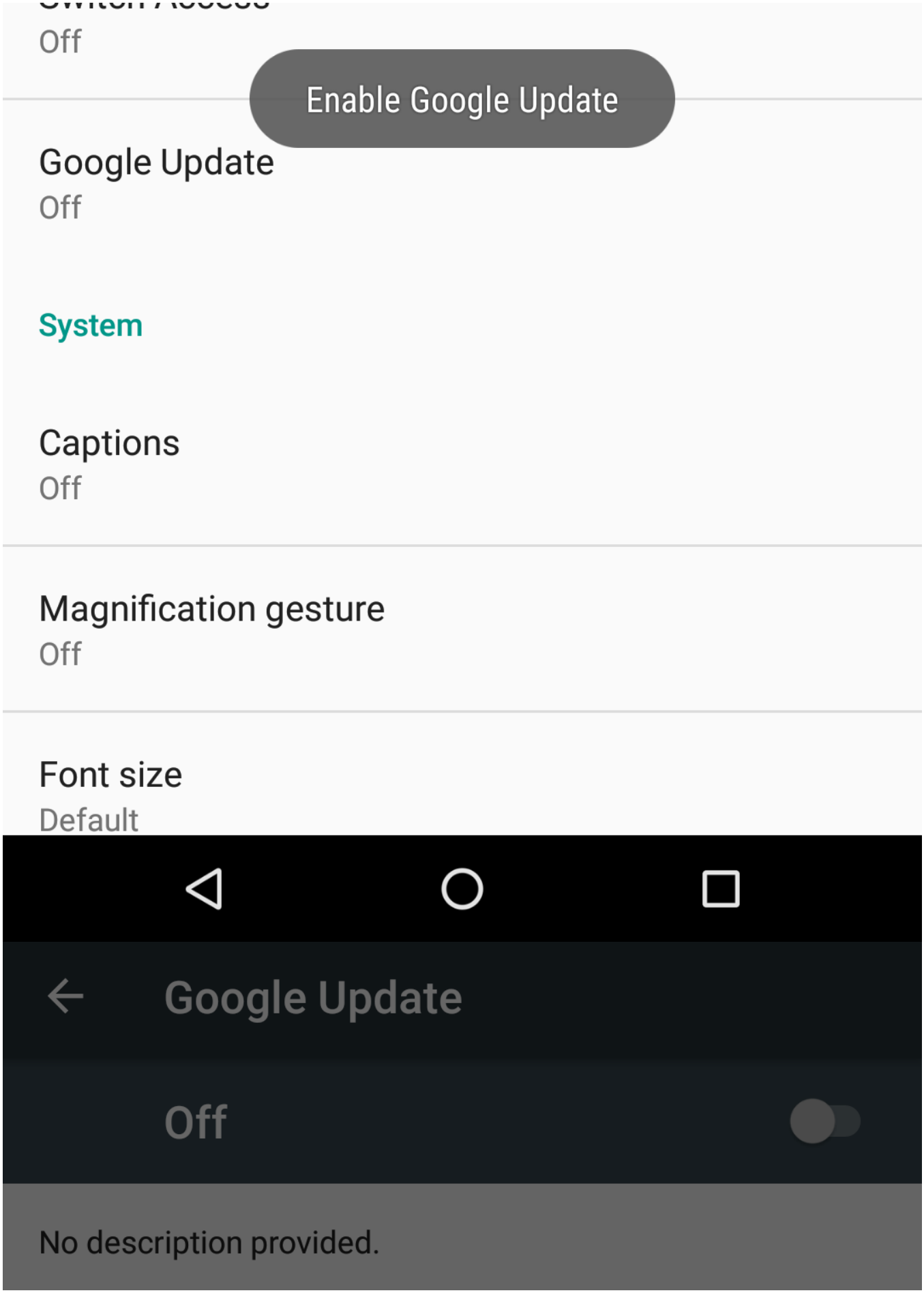
enhanced with accessibility features and some automated scripts (such as PayPal automated transfer scripts). In May 2019 the Xerxes Trojan first appeared, it was based on Parasite and after some unsuccessful attempts in offering the Trojan in underground forums, the actor made it publicly available. After being used by several actors, it faded away from the threat landscape. In May 2020 BlackRock was first spotted.

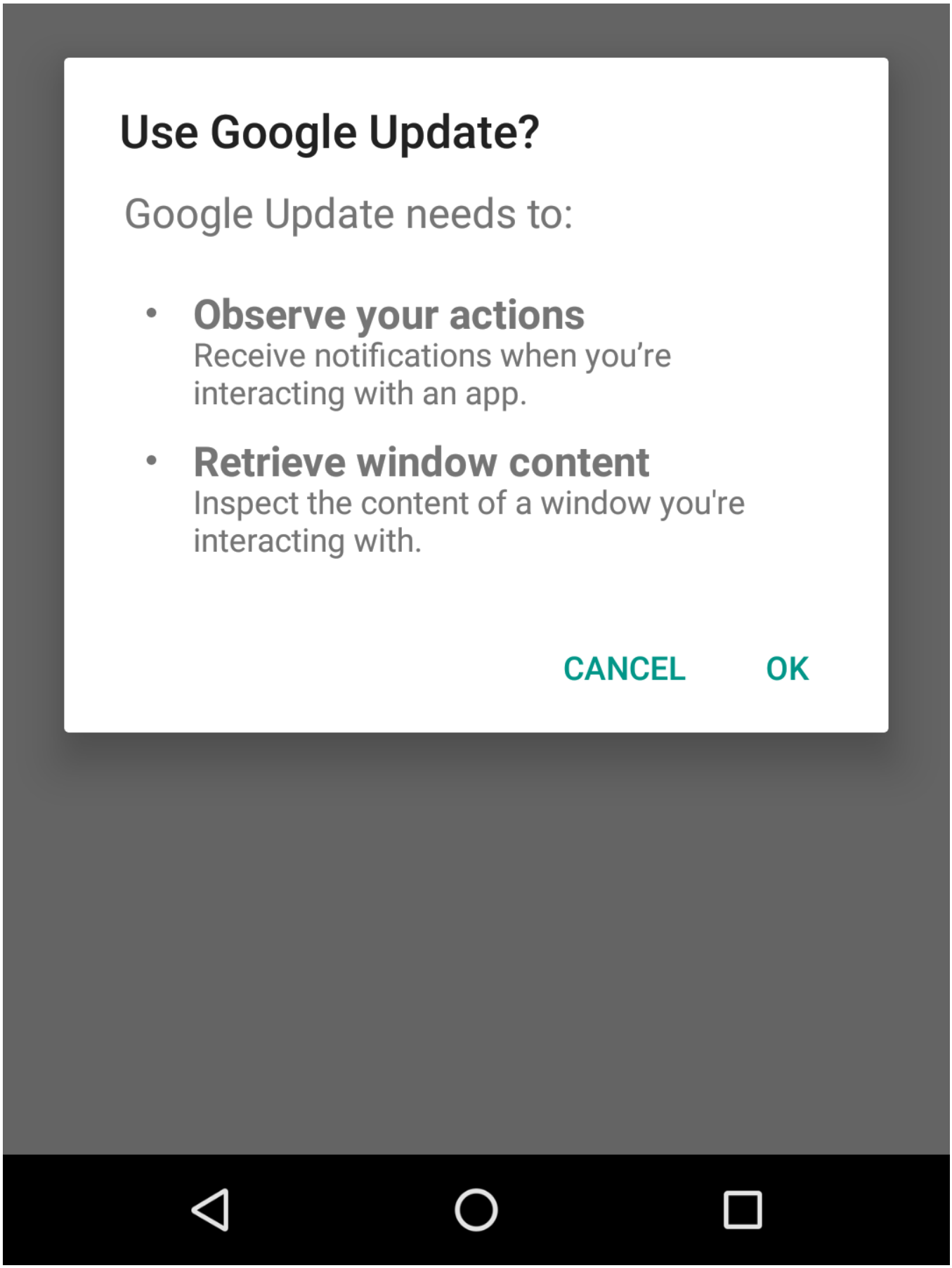


How it works

When the malware is first launched on the device, it will start by hiding its icon from the app drawer, making it invisible to the end-user. As second step it asks the victim for the Accessibility Service privileges. As visible in following screenshot, the Trojan's largest campaigns are posing as fake Google updates:




Off
Enable Google Update
Google Update
Off
System
Captions
Off
Magnification gesture
Off
Font size
Default
Google Update
Off
No description provided.



Once the user grants the requested Accessibility Service privilege, BlackRock starts by granting itself additional permissions. Those additional permissions are required for the bot to fully function without having to interact any further with the victim. When done, the bot is functional and ready to receive commands from the C2 server and perform the overlay attacks.

Commands

The commands supported by the actual version of the bot are listed below. It gives a good overview of what the actor(s) can do on the infected device.

Command	Description
Send_SMS	Sends an SMS
Flood_SMS	Sends an SMS to a specific number every 5 seconds
Download_SMS	Sends a copy of SMS messages to C2
Spam_on_contacts	Sends an SMS to each of the contacts present on the infected device
Change_SMS_Manager	Set malware as default SMS manager (command is repeated every 30 seconds until action is achieved)
Run_App	Starts a specific app on the bot
StartKeyLogs	Logs text content shown on the screen from targets and sends it to the C2
StopKeyLogs	Stops logging the accessibility events from targets
StartPush	Send a copy of all notifications content to the C2
StopPush	Stops sending a copy of all notifications content to the C2
Hide_Screen_Lock	Keeps the device on the HOME screen
Unlock_Hide_Screen	Unlocks the device from the HOME screen
Admin	Makes the both request admin privileges
Profile	Adds a managed admin profile for the malware on the device
Start_clean_Push	Dismisses (hiding) all push notifications
Stop_clean_Push	Stops dismissing push notifications

Features

BlackRock offers a quite common set of capabilities compared to average Android banking Trojans. It can perform the infamous overlay attacks, send, spam and steal SMS messages, lock the victim in the launcher activity (HOME screen of the device), steal and hide notifications, deflect usage of Antivirus software on the device and act as a keylogger. Interestingly, the Xerxes Trojan itself offers more features, but it seems that actors have removed some of them in order to only keep those that they consider useful to steal personal information.

The keylogger logs the text content from apps shown on the screen and will do so for applications included in the targets lists only.

The Trojan will redirect the victim to the HOME screen of the device if the victims tries to start or use antivirus software as per a specific list including Avast, AVG, BitDefender, Eset, Symantec, TrendMicro, Kaspersky, McAfee, Avira, and even applications to clean Android devices, such as TotalCommander, SD Maid or Superb Cleaner. By doing so, the Trojan tries to avoid letting the victim remove it from the device and establish some form of persistency.

BlackRock embeds following set of features, allowing it to remain under the radar and successfully harvest personal information:

- Overlaying: Dynamic (Local injects obtained from C2)
- Keylogging
- SMS harvesting: SMS listing
- SMS harvesting: SMS forwarding
- Device info collection
- SMS: Sending
- Remote actions: Screen-locking
- Self-protection: Hiding the App icon
- Self-protection: Preventing removal
- Notifications collection
- Grant permissions
- AV detection

Profiling

One functionality that is so far unique to BlackRock is that it makes usage of the Android work profiles. This Android feature is usually used by companies to define a device policy controller (DPC) in order to control and apply policies on their mobile fleet. It allows to control various aspects of a device without per se having complete administration rights on all aspects of the device.

BlackRock abuses this feature to gain admin privileges. It simply creates and attributes itself a profile which has the admin privileges.

The following code snippet show how the profile is created:

```
private void createProfile() {
    try {
        Intent intent = new Intent("android.app.action.PROVISION\_MANAGED\_PROFILE");
        if(Build.VERSION.SDK_INT < 23) {
            intent.putExtra("android.app.extra.", this.getApplicationContext().getPackageName());
        }
        else {
            intent.putExtra("android.app.extra.PROVISIONING\_DEVICE\_ADMIN\_COMPONENT\_NAME", new ComponentName(this,
Admins.class.getName()));
        }

        if(intent.resolveActivity(this.getPackageManager()) != null) {
            this.startActivityForResult(intent, 101);
            return;
        }
    }
    catch(Exception e) {
        e.printStackTrace();
        return;
    }
}
```

Overlay attack

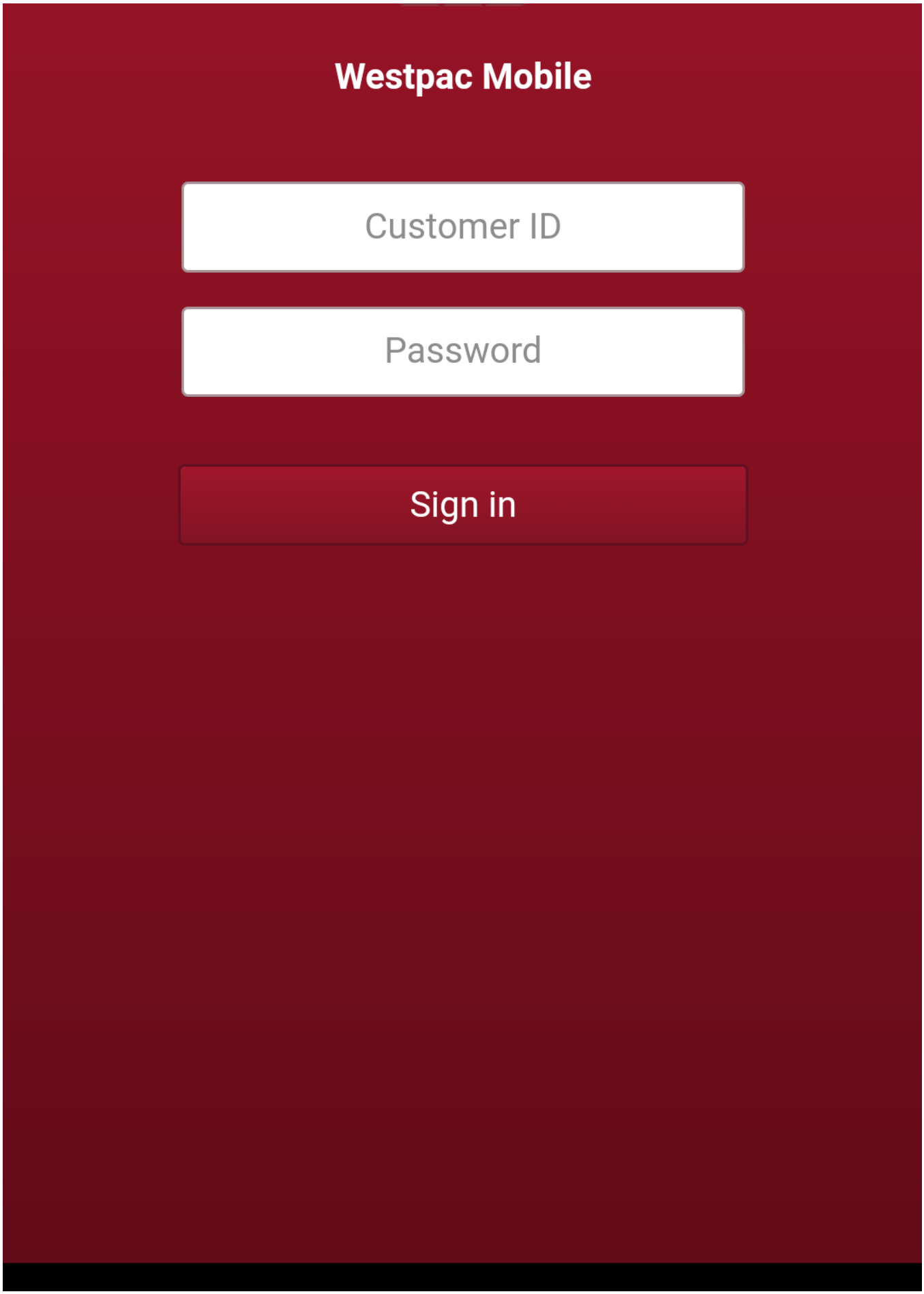
BlackRock abuses the Accessibility Service to check which application runs in the foreground. Like the Ginp Android banking Trojan, BlackRock has two types of overlay screens, one is a generic card grabber view and the other is specific per targeted app - credential phishing overlay. Both target lists can be found in the appendix of this blog.

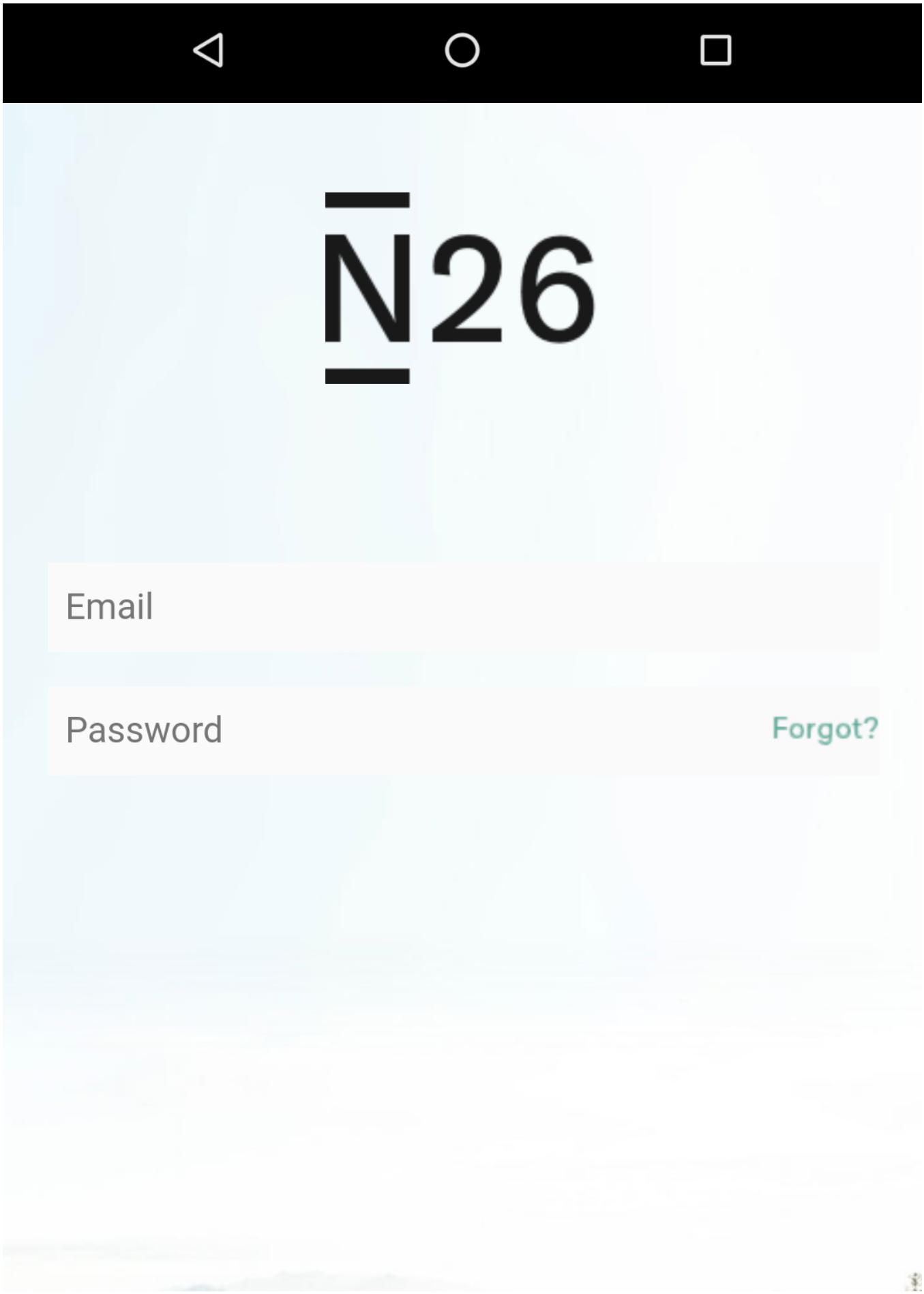
The following code snippet shows how the overlay WebView is created:

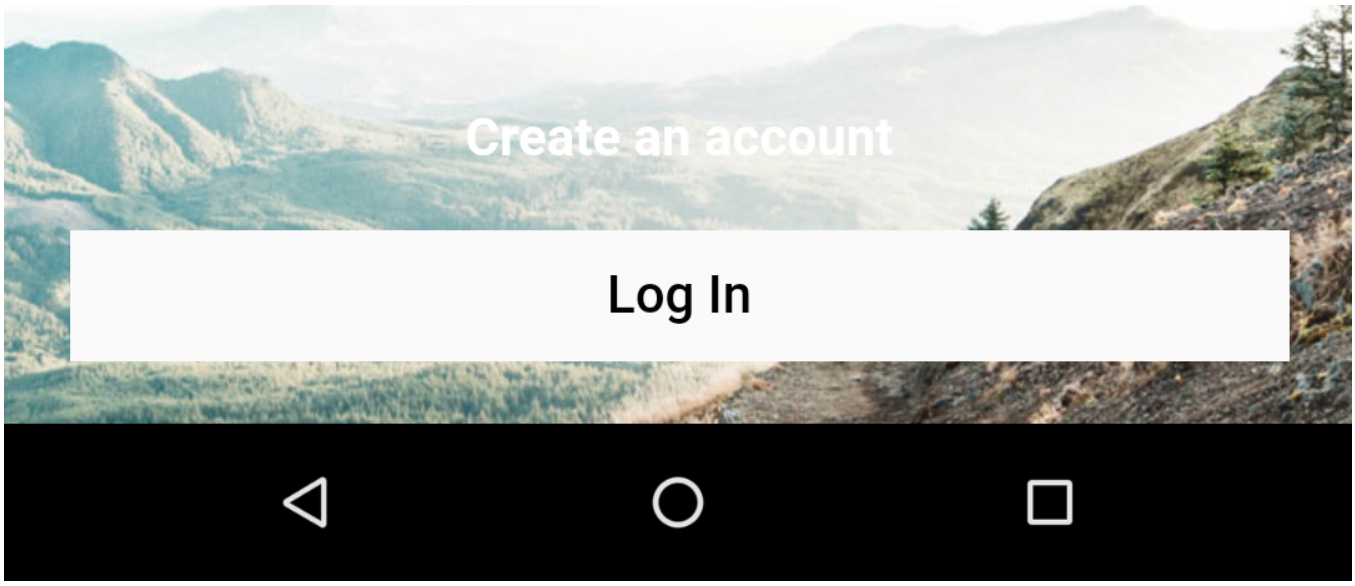
```
protected void onStart() {
    super.onStart();
    SharedPreferences.Editor editor = PreferenceManager.getDefaultSharedPreferences(this).edit();
    editor.putBoolean("injActive", true);
    editor.commit();
    String packageName = this.getIntent().getStringExtra("str");
    String injURL = this.getFilesDir().getAbsolutePath() + File.separator;
    try {
        this.webView = new WebView(this);
        this.webView.getSettings().setJavaScriptEnabled(true);
        this.webView.setScrollBarStyle(0);
        this.webView.setWebChromeClient(new WebChromeClient());
        this.webView.addJavascriptInterface(new JSInterface(this, packageName), "Android");
        this.webView.setWebViewClient(new Inject.a(this));
        this.webView.loadUrl("file:///" + injURL + packageName + "/index.html");
        this.setContentView(this.webView);
        this.webView.setWebViewClient(new Inject.b(this, packageName));
    }
    catch(Exception e) {
        e.printStackTrace();
    }
}
```

As shown in the previous code snippet, the URL of the overlay points to local files rather than a web location. This is a feature that is inherited from Xerxes, which downloads an archive with all the targets overlays files on the infected device. BlackRock does it somehow differently by downloading a separate archive for each targeted app installed on the device.

Following screenshots show some of the credential phishing overlays:


Westpac Mobile
Customer ID
Password
Sign in


N26
Email
Password
Forgot?



Royal Bank of Scotland

Step 1 of 3

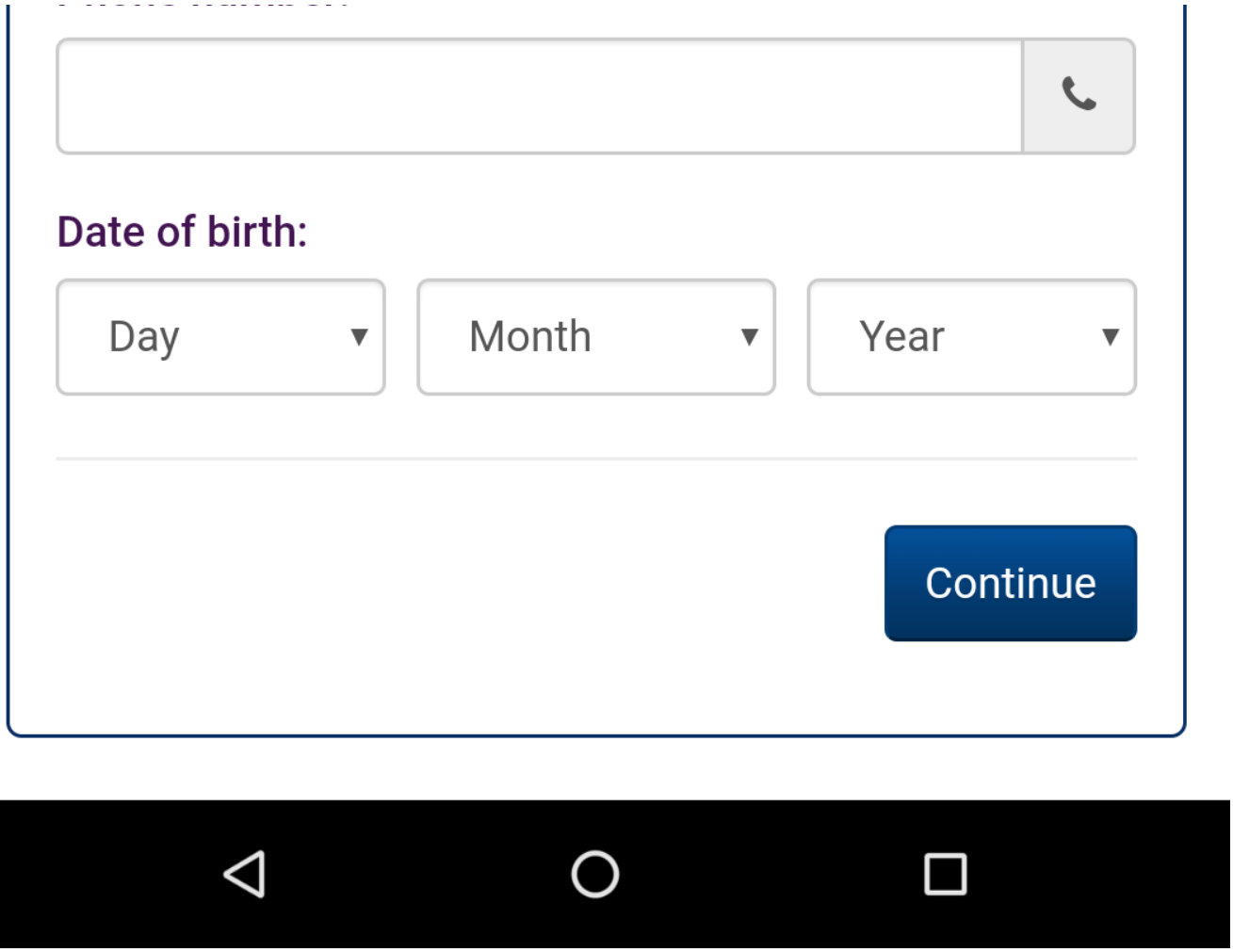
Attention

For security reasons you must confirm your identity. Please note providing wrong or invalid information could lead to account suspension..

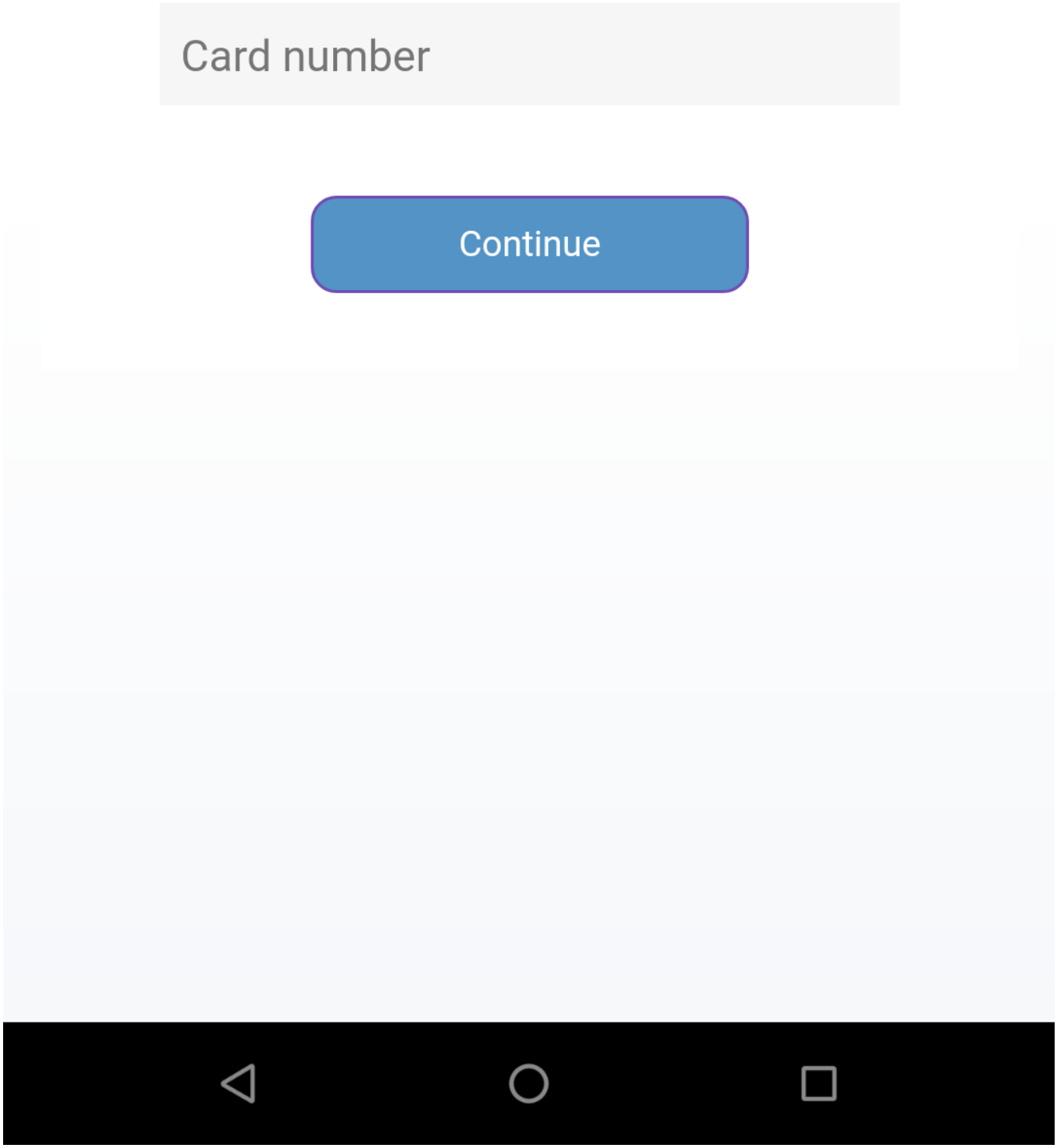
First name:

Last name:

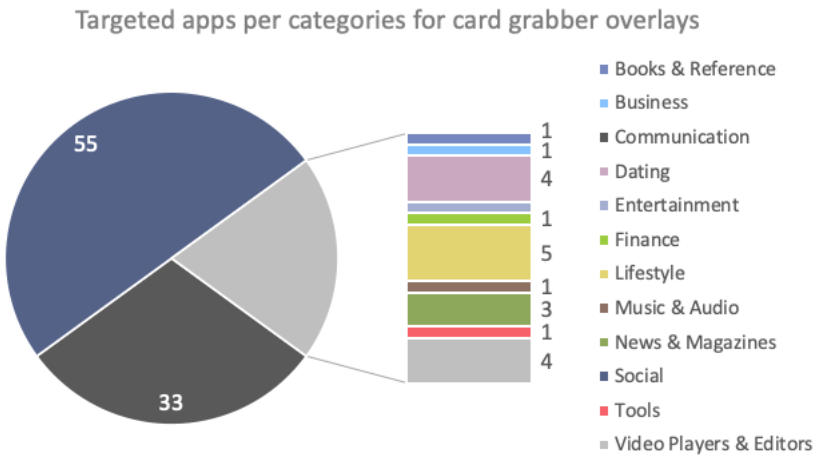
Phone number:



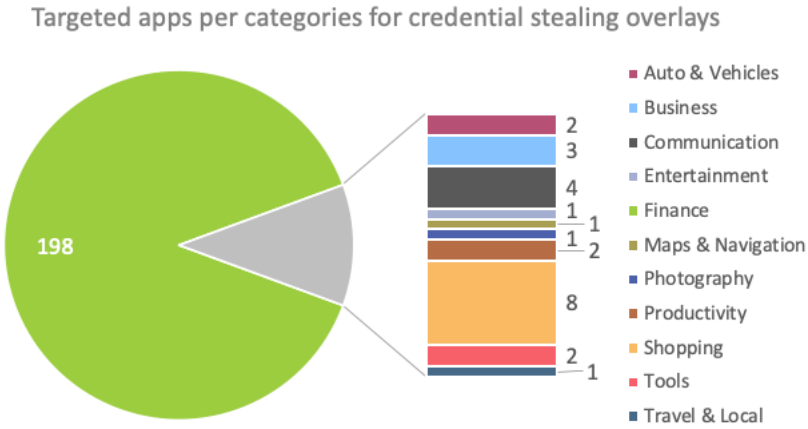
Following screenshot shows the generic card grabber overlay:



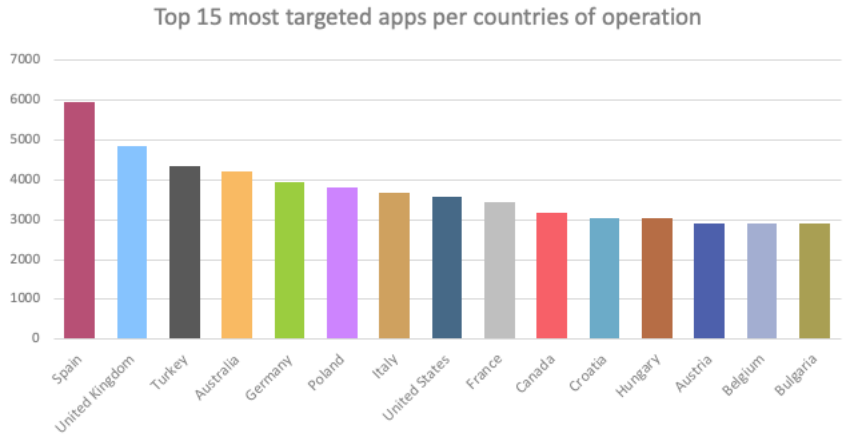
Interestingly, of the 337 unique applications in BlackRock's target lists, many applications haven't been observed to be targeted by banking malware before. Those "new" targets are mostly not related to financial institutions and are overlayed in order to steal credit card details. As shown in the following chart, most of the non-financial apps are Social, Communication, Lifestyle and Dating apps. Most of the trending social and dating apps are included, the actors' choice might have been driven by the pandemic situation, pushing people to socialized more online. It also seems that actors have made a particular effort on including dating apps, which wasn't something common in targets list so far.



When it comes to the targets of the credential-stealing overlays, the majority of the most targeted apps are related to banks operating in Europe, followed by Australia, the United States of America and Canada. But financial apps are not the only ones included in the list; shopping, communication and business apps seem to have a certain interest for the actors. Among others, we found some applications related to German online car selling services, Polish online shopping sites and well-known email services. The following chart shows the ratio of targeted apps per app category.



As visible in following chart, the BlackRock Trojan's target list includes applications operating in a variety of different countries. The chart shows the number of occurrences of financial apps per countries of operation for all BlackRock samples observed so far.



Conclusion

Although we've observed a steady increase in the number of new banking Trojans since 2014, 2020 shows an interesting increase again after a quite calm 2019. As stated in our blog 2020 - Year of the RAT not only are there more new Android banking Trojans, but some of them also bring innovative new features. Most of them start embedding features, allowing the criminals to take remote control of the infected device

(RAT) and sometimes even to automatically perform the fraud from the infected device (ATS). In the case of BlackRock, the features are not very innovative but the target list has a large international coverage and it contains quite a lot of new targets which haven't been seen being targeted before.

Although BlackRock poses a new Trojan with an exhaustive target list, looking at previous unsuccessful attempts of actors to revive LokiBot through new variants, we can't yet predict how long BlackRock will be active on the threat landscape. What can be considered as true is that the number of new banking Trojans will continue to grow, bringing new functionalities to increase the success rate of fraud while fraud becomes a growing risk even for consumers not using mobile banking - as we can see with BlackRock targeting 3rd party apps.

The second half of 2020 will come with its surprises, after Alien, Eventbot and BlackRock we can expect that financially motivated threat actors will build new banking Trojans and continue improving the existing ones. With the changes that we expect to be made to mobile banking Trojans, the line between banking malware and spyware becomes thinner, banking malware will pose a threat for more organizations and their infrastructure, an organic change that we observed on windows banking malware years ago.

The most important aspect to take care of is securing the online banking channels, making fraud hard to perform, therefore discouraging criminals to make more malware.

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 BlackRock samples found in the wild:

App name	Package name	SHA-256 hash
Google Update	ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplb	51f9c37c3eec0b6f8325aa1c8fe64a0615ab920584042df557426473b1
Google Update	cmbmpqod.bfrtuduawoyhr.mlmrncmjbdecuc	6fa4baef8a811f429cee4b383d7a4776b7b363b62551c8d8e0f93bad33
Google Update	fpjwhqsl.dzpycoeasyhs.cwnporwocambskrxcxiug	7d34aaf84754fb247507681bcd821f9533f24c6d78aa6779a11f4d789d
Google Update	onpekpikylb.bcgdhxgzwd.dzlecjglpigjuc	81fda9ff99aec1b6f7b328652e330d304fb18ee74e0dbd0b759acb24e7
Google Update	ezmjhdiumgiyhfjdp.bjucshsqxhkigwyqqma.gqncehdcknrtcekingi	fbaf785edfafa583ea61884d88f507a27154892a394e27d81102f79fe7e

Credential theft target list

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

App name	Package name
TransferWise Money Transfer	com.transferwise.android
PayPal Mobile Cash: Send and Request Money Fast	com.paypal.android.p2pmobile
Payoneer – Global Payments Platform for Businesses	com.payoneer.android
NETELLER - fast, secure and global money transfers	com.moneybookers.skrillpayments.neteller
EO.Finance: Buy and Sell Bitcoin. Crypto Wallet	com.eofinance
Azimo Money Transfer	com.azimo.sendmoney

App name	Package name
ePayments: wallet & bank card	clientapp.swiftcom.org
Yahoo Mail – Organized Email	com.yahoo.mobile.client.android.mail
Microsoft Outlook: Organize Your Email & Calendar	com.microsoft.office.outlook
mail.com mail	com.mail.mobile.android.mail
Gmail	com.google.android.gm
Google Play services	com.google.android.gms
Connect for Hotmail & Outlook: Mail and Calendar	com.connectivityapps.hotmail
Uber - Request a ride	com.ubercab
Netflix	com.netflix.mediaclient
eBay: Buy, sell, and save money on home essentials	com.ebay.mobile
Amazon Seller	com.amazon.sellermobile.android
Amazon Shopping - Search, Find, Ship, and Save	com.amazon.mShop.android.shopping
Skrill - Fast, secure online payments	com.moneybookers.skrillpayments
Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum	piuk.blockchain.android
Bitcoin Wallet Coincheck	jp.coincheck.android
Ethos Universal Wallet	io.ethos.universalwallet
Indodax	id.co.bitcoin
WazirX - Buy Sell Bitcoin & Other Cryptocurrencies	com.wrx.wazirx
Unocoin Wallet	com.unocoin.unocoinwallet
Cash App	com.squareup.cash
Bitcoin Wallet - Buy BTC	com.polehin.android
Plus500: CFD Online Trading on Forex and Stocks	com.Plus500
PAYEER	com.payeer
Paxful Bitcoin Wallet	com.paxful.wallet
Paribu	com.paribu.app
Mycelium Bitcoin Wallet	com.mycelium.wallet
EXMO Official - Trading crypto on the exchange	com.exmo
Coinbase – Buy & Sell Bitcoin. Crypto Wallet	com.coinbase.android
BtcTurk Bitcoin Borsası	com.btcturk
BitPay – Secure Bitcoin Wallet	com.bitpay.wallet
Aplikacja Bitmarket	com.bitmarket.trader
Bitfinex	com.bitfinex.mobileapp
Binance - Buy & Sell Bitcoin Securely	com.binance.dev
Bitcoin Wallet - Airbitz	com.airbitz
Edge - Bitcoin, Ethereum, Monero, Ripple Wallet	co.edgesecure.app
bitbank - Bitcoin & Ripple Wallet	cc.bitbank.bitbank
Bank of Scotland Business Mobile Banking	uk.co.bankofscotland.businessbank
Westpac Mobile Banking	org.westpac.bank
BankSA Mobile Banking	org.banksa.bank

App name	Package name
St.George Tablet Banking	org.banking.tablet.stgeorge
Mes Comptes BNP Paribas	net.bnpparibas.mescomptes
Santander Mobile Banking	mobile.santander.de
Speedway Fuel & Speedy Rewards	com.speedway.mobile
RBS Investor & Media Relations	com.rbs.mobile.investisir
Ulster Bank RI Mobile Banking	com.rbs.mobile.android.ubr
RBS Business Banking	com.rbs.mobile.android.rbsbandc
Royal Bank of Scotland Mobile Banking	com.rbs.mobile.android.rbs
NatWest International	com.rbs.mobile.android.natwestoffshore
NatWest Business Banking	com.rbs.mobile.android.natwestbandc
NatWest Mobile Banking	com.rbs.mobile.android.natwest
RBS	com.phyder.engage
Lloyds Bank Business Mobile Banking	com.lloydsbank.businessmobile
ING-DiBa Banking + Brokerage	com.ing.diba.mbbr2
TSBBank Mobile Banking	com.ifs.banking.fiid4202
BANKWEST OF KANSAS	com.ifs.banking.fiid3767
HSBC Mobile Banking	com.htsu.hsbcpersonalbanking
Bank of Scotland Mobile Banking: secure on the go	com.grppl.android.shell.BOS
Garanti CepBank	com.garanti.cepbank
TSB Mobile	com.fi6122.godough
Volume Control +	com.cb.volumePlus
Barclays	com.barclays.android.barclaysmobilebanking
ANZ Spot	com.anzspot.mobile
-	com.anz.SingaporeDigitalBanking
ANZ Mobile Taiwan	com.anz.android
Akbank Direkt Şifreci	com.akbank.softotp
Garanti BBVA Cep Şifrematik	biz.mobinex.android.apps.cep_sifrematik
ING España. Banca Móvil	www.ingdirect.nativeframe
BROU Llave Digital	uy.com.brou.token
App Móvil del Banco República	uy.brou
TSB Mobile Banking	uk.co.tsb.newmobilebank
Santander Mobile Banking	uk.co.santander.santanderUK
HSBC UK Mobile Banking	uk.co.hsbc.hsbcukmobilebanking
ŞEKER MOBİL ŞUBE	tr.com.sekerbilisim.mbank
HSBC Turkey	tr.com.hsbc.hsbcturkey
PeoPay	softax.pekao.powerpay
Postepay	posteitaliane.posteapp.apppostepay
IKO	pl.pkobp.iko
Mój Orange	pl.orange.mojeorange

App name	Package name
mBank PL	pl.mbank
Moje ING mobile	pl.ing.mojeing
IFIRMA - Darmowy Program do Faktur	pl.ifirma.ifirmafaktury
Fakturownia.pl	pl.fakturownia
Rossmann PL	pl.com.rossmann.centauros
Ceneo - zakupy i promocje	pl.ceneo
Santander mobile	pl.bzwbk.bzwbk24
Allegro - convenient and secure online shopping	pl.allegro
Erste MobilBank	pegasus.project.ebh.mobile.android.bundle.mobilebank
Interbank APP	pe.com.interbank.mobilebanking
St.George Mobile Banking	org.stgeorge.bank
Banco Sabadell App. Your mobile bank	net.inverline.bancosabadell.officelocator.android
Maybank2u MY	my.com.maybank2u.m2umobile
L'Appli Société Générale	mobi.societegenerale.mobile.lappli
Pocket Bank	ma.gbp.pocketbank
楽天銀行 -個人のお客様向けアプリ	jp.co.rakuten_bank.rakutenbank
SCRIGNOapp	it.popso.SCRIGNOapp
UBI Banca	it.nogood.container
ING Italia	it.ingdirect.app
Banca MPS	it.copergmps.rt.pf.android.sp.bmps
BNL	it.bnl.apps.banking
MKB Mobilalkalmazás	hu.mkb.mobilapp
Erste Business MobilBank	hu.cardinal.erste.mobilapp
CIB Business Online	hu.cardinal.cib.mobilapp
Budapest Bank Mobil App	hu.bb.mobilapp
Bi en Línea	gt.com.bi.bienlinea
Mes Comptes - LCL	fr.lcl.android.customerarea
Ma Banque	fr.creditagricole.androidapp
Banque Populaire	fr.banquepopulaire.cyberplus
Enpara.com Cep Şubesi	finansbank.enpara
HVB Mobile Banking	eu.unicreditgroup.hvbapptan
PekaoBiznes24	eu.eleader.mobilebanking.pekao.firm
Pekao24Makler	eu.eleader.mobilebanking.pekao
plusbank24	eu.eleader.mobilebanking.invest
UnicajaMovil	es.univia.unicajamovil
Pibank	es.pibank.customers
Openbank – banca móvil	es.openbank.mobile
Banca Digital Liberbank	es.liberbank.cajasturapp
CaixaBank	es.lacaixa.mobile.android.newwapicon

App name	Package name
Ibercaja	es.ibercaja.ibercajaapp
EVO Banco móvil	es.evobanco.bancamovil
Bankia	es.cm.android
Cajalnet	es.ceca.cajalnet
Banco Caixa Geral España	es.caixageral.caixageralapp
ABANCA- Banca Móvil	es.caixagalicia.activamovil
Santander Empresas	es.bancosantander.empresas
tractorpool	de.traktorpool
Postbank Finanzassistent	de.postbank.finanzassistent
N26 — The Mobile Bank	de.number26.android
mobile.de – Germany‘s largest car market	de.mobile.android.app
ING Banking to go	de.ingdiba.bankingapp
VR Banking Classic	de.fiducia.smartphone.android.banking.vr
DKB-Banking	de.dkb.portalapp
Consorsbank	de.consorsbank
Commerzbank Banking - The app at your side	de.commerzbanking.mobil
comdirect mobile App	de.comdirect.android
Banco Santander Perú S.A.	com.zoluxiones.officebanking
Ziraat Mobile	com.ziraat.ziraatmobil
Yapı Kredi Mobile	com.ykb.android
Wells Fargo Mobile	com.wf.wellsfargomobile
VakıfBank Mobil Bankacılık	com.vakifbank.mobile
-	com.uy.itau.appitauuypfcom.usbank.mobilebankingcom.usaa.mobile.android.usaa
Mobile Banking UniCredit	com.unicredit
Halkbank Mobil	com.tmobtech.halkbank
Tide - Smart Mobile Banking	com.tideplatform.banking
Banca Móvil Laboral Kutxa	com.tecnocom.cajalaboral
CEPTETEB	com.teb
TARGOBANK Mobile Banking	com.targo_prod.bad
SunTrust Mobile App	com.suntrust.mobilebanking
Sparkasse Ihre mobile Filiale	com.starfinanz.smob.android.sfinanzstatus
IDBI Bank GO Mobile+	com.snapwork.IDBI
SCB EASY	com.scb.phone
Yono Lite SBI - Mobile Banking	com.sbi.SBIFreedomPlus
Santander Private Banking	com.santander.bpi
ruralvía	com.rsi
RBC Mobile	com.rbc.mobile.android
Liquid by Quoineライト版（リキッドバイコイン） -ビットコインなどの仮想通貨取引所	com.quoine.quoinex.light

App name	Package name
PTTBank	com.pttfinans
İşCep - Mobile Banking	com.pozitron.iscep
Bill Payment & Recharge,Wallet	com.oxigen.oxigenwallet
Papara	com.mobillium.papara
BHIM UPI, Money Transfer, Recharge & Bill Payment	com.mobikwik_new
Odeabank	com.magiclick.odeabank
YouApp	com.lynxspa.bancopopolare
Intesa Sanpaolo Mobile	com.latuabancaperandroid
Kuveyt Türk	com.kuveytturk.mobil
Kutxabank	com.kutxabank.android
KMA	com.krungsri.kma
Capital One® Mobile	com.konylabs.capitalone
K PLUS	com.kasikorn.retail.mbanking.wap
ING France	com.IngDirectAndroid
ING Mobil	com.ingbanktr.ingmobil
Bank of America Mobile Banking	com.infonow.bofa
Triodos Bank. Banca Móvil	com.indra.itecban.triodosbank.mobile.banking
NBapp Spain	com.indra.itecban.mobile.novobanco
imaginBank - Your mobile bank	com.imaginbank.app
בנק הפועלים - ניהול החשבון	com.ideomobile.hapoalim
Grupo Cajamar	com.grupocajamar.wefferent
Halifax: the banking app that gives you extra	com.grppl.android.shell.halifax
Lloyds Bank Mobile Banking: by your side	com.grppl.android.shell.CMBlloydsTSB73
ビットコイン・暗号資産（仮想通貨）ウォレットアプリ GMOコイン｜チャート・購入・レバレッジ取引	com.gmowallet.mobilewallet
Garanti BBVA Mobile	com.garanti.cepsubesi
CA24 Mobile	com.finanteq.finance.ca
Empik Foto	com.empik.empikfoto
Empik	com.empik.empikapp
Discover Mobile	com.discoverfinancial.mobile
MobilDeniz	com.denizbank.mobildeniz
Deutsche Bank Mobile	com.db.pwcc.dbmobile
Mi Banco db	com.db.pbc.mibanco
La Mia Banca	com.db.pbc.miabanca
norisbank App	com.db.mm.norisbank
iMobile by ICICI Bank	com.csam.icici.bank.imobile
CommBank	com.commbank.netbank
Crédit Mutuel	com.cm_prod.bad
Fifth Third Mobile Banking	com.clairmail.fth

App name	Package name
CIMB Clicks Malaysia	com.cimbmalaysia
CIBC Mobile Banking®	com.cibc.android.mobi
Chase Mobile	com.chase.sig.android
Cajasur	com.cajasur.android
Banque	com.caisseepargne.android.mobilebanking
Boursorama Banque	com.boursorama.android.clients
BMO Mobile Banking	com.bmo.mobile
Banca Móvil BCP	com.bcp.bank.bcp
BBVA Perú	com.bbva.nxt_peru
BBVA Net Cash | ES & PT	com.bbva.netcash
BBVA Spain	com.bbva.bbvacontigo
Bankinter Móvil	com.bankinter.launcher
Bankinter Empresas	com.bankinter.empresas
myAT&T	com.att.myWireless
AmOnline	com.ambank.ambankonline
Albaraka Mobile Banking	com.albarakaapp
Akbank	com.akbank.android.apps.akbank_direkt
OTP SmartBank	com.aff.otpdirekt
ABN AMRO Mobiel Bankieren	com.abnamro.nl.mobile.payments
ABANCA Empresas	com.abanca.bancaempresas
Invoice Maker: Estimate & Invoice App	com.aadhk.woinvoice
AutoScout24 Switzerland – Find your new car	ch.autoscout24.autoscout24
NAB Mobile Banking	au.com.nab.mobile
ING Australia Banking	au.com.ingdirect.android
WiZink, tu banco senZillo	app.wizink.es
Usługi Bankowe	alior.bankingapp.android
QNB Finansbank Mobile Banking	com.finansbank.mobile.cepsube

Credit Card theft target list

The actual BlacRock target list used for credit card theft contains 111 applications:

App name	Package name
Telegram	org.telegram.messenger
Viber Messenger - Messages, Group Chats & Calls	com.viber.voip
WhatsApp Messenger	com.whatsapp
WhatsApp Business	com.whatsapp.w4b
Twitter	com.twitter.android
Twitter Lite	com.twitter.android.lite
Snapchat	com.snapchat.android
Skype - free IM & video calls	com.skype.raider

App name	Package name
Skype Lite - Free Video Call & Chat	com.skype.m2
Skype for Business for Android	com.microsoft.office.lync15
Instagram	com.instagram.android
imo free video calls and chat	com.imo.android.imoim
imo beta free calls and text	com.imo.android.imoimbeta
imo HD-Free Video Calls and Chats	com.imo.android.imoimhd
Messenger – Text and Video Chat for Free	com.facebook.orca
Facebook	com.facebook.katana
Messenger Lite: Free Calls & Messages	com.facebook.mlite
Facebook Lite	com.facebook.lite
Play Store	com.android.vending
PlayStation Messages - Check your online friends	com.playstation.mobilemessenger
Uplive - Live Video Streaming App	com.asiainno.uplive
Fiesta by Tango - Find, Meet and Make New Friends	com.sgiggle.mango
Hoop - New friends on Snapchat	com.dazz.hoop
LivU: Meet new people & Video chat with strangers	com.videochat.livu
MICO Chat: Make New Friends & Live Chat	com.mico
Crowdfire: Social Media Manager	com.justunfollow.android
SKOUT - Meet, Chat, Go Live	com.skout.android
LP: Live Stream Video Dating & Chat	ru.loveplanet.app
Surge: Gay Dating & Chat	com.lavendrapp.lavendr
LOVELY – Your Dating App To Meet Singles Nearby	com.pinkapp
VK — live chatting & free calls	com.vkontakte.android
Amberfog for VK	com.amberfog.vkfree
V LIVE	com.naver.vapp
We Heart It	com.weheartit
Video Chat W-Match : Dating App, Meet & Video Chat	com.waplogmatch.social
Reddit	com.reddit.frontpage
Tango - Live Video Broadcasts	com.sgiggle.production
JAUMO Dating – Flirt With Local Singles	com.jaumo
Free Dating	com.mobile.android.eris
Topface - Dating Meeting Chat	com.topface.topface
DISCO 🏳️‍🌈 Gay Dating & Gay Chat for Homosexuals	com.jaumo.gay
Mail.Ru Dating	ru.mail.love
Airtripp:Free Foreign Chat	com.taptrip
Amino Anime Russian аниме и манга	com.narvii.amino.x156542274
Bigo Live - Live Stream, Live Video & Live Chat	sg.bigo.live
BIGO LIVE Lite – Live Stream	sg.bigo.live.lite
Waplog - Dating App to Chat & Meet New People	com.waplog.social

App name	Package name
SPICY 🌶 Lesbian Chat & Dating	com.jaumo.lesbian
VK Live	com.vk.stream
Periscope - Live Video	tv.periscope.android
Hornet - Gay Social Network	com.hornet.android
My World. Movies. Games	ru.mail.my
Tumblr	com.tumblr
Badoo — Dating App to Chat, Date & Meet New People	com.badoo.mobile
BLOOM — Premium Dating & Find Real Love	com.jaumo.prime
IGTV	com.instagram.igtv
Ночной ВК	com.amberfog.reader
Galaxy - Chat Rooms: Meet New People Online & Date	ru.mobstudio.andgalaxy
Amino: Communities and Chats	com.narvii.amino.master
ASKfm - Ask Me Anonymous Questions	com.askfm
Kate Mobile for VK	com.perm.kate_new_6
F3 - Make new friends, Anonymous questions, Chat	cool.f3
All social media and social networks in one app	com.web_view_mohammed.ad.webview_app
Анонимный чат NektoMe	com.nektome.talk
Pinterest	com.pinterest
Get new friends on local chat rooms	drug.vokrug
OK	ru.ok.android
Mamba - Online Dating App: Find 1000s of Single	ru.mamba.client
Google Play Books - Ebooks, Audiobooks, and Comics	com.google.android.apps.books
Google Play Music	com.google.android.music
Google Play Movies & TV	com.google.android.videos
Hangouts	com.google.android.talk
Google Pay: Pay with your phone and send cash	com.google.android.apps.walletnfcrel
Catfiz Messenger	com.catfiz
Tabor - Знакомства	ru.tabor.search
Video Downloader for TikTok - TikMate	tikmate.tiktokvideodownloader.savetiktokvideo.nowatermark
TikTok - Make Your Day	com.zhiliaoapp.musically
TikTok Lite	com.zhiliaoapp.musically.go
WeChat	com.tencent.mm
ClonApp - Dual Messenger for WhatsApp Story Saver	com.bluesoft.clonappmessenger
Glide - Video Chat Messenger	com.glidetalk.glideapp
Telegram X	org.thunderdog.challegram
KakaoTalk: Free Calls & Text	com.kakao.talk
SOMA free video call and chat	com.instanza.baba
BiP – Messaging, Voice and Video Calling	com.turkcell.bip
Vidogram	org.vidogram.messenger

App name	Package name
BGram	org.telegram.BifToGram
Graph Messenger	ir.ilmili.telegraph
Kik	kik.android
Messenger Messenger Messenger	messenger.pro.messenger
free video calls and chat	ru.mail
Faster for Facebook	com.nbapstudio.facebooklite
Messenger	com.aleskovacic.messenger
Pinngle Safe Messenger: Free Calls & Video Chat	com.beint.pinngle
Social Messenger: Free Mobile Calling, Live Chats	com.messagingnew.allinone
ICQ New: Instant Messenger & Group Video Calls	com.icq.mobile.client
Plus Messenger	org.telegram.plus
TamTam Messenger - free chats & video calls	ru.ok.messages
Coco	com.instanza.cocovoice
Messenger	messenger.social.chat.apps
Fast for Facebook & Messenger	com.messenger.superiorstudio
Azar	com.azarlive.android
Bermuda Video Chat - Meet New People	vixr.bermuda
Fachat: Video Chat with New People Online	com.fachat.freechat
MeetMe: Chat & Meet New People	com.myyearbook.m
OK Live - video livestreams	ru.ok.live
Tinder	com.tinder
Tumile - Meet new people via free video chat	com.rcplatform.livechat
Blued - LIVE Gay Dating, Chat & Video Call to Guys	com.blued.international
Grindr - Gay chat	com.grindrapp.android