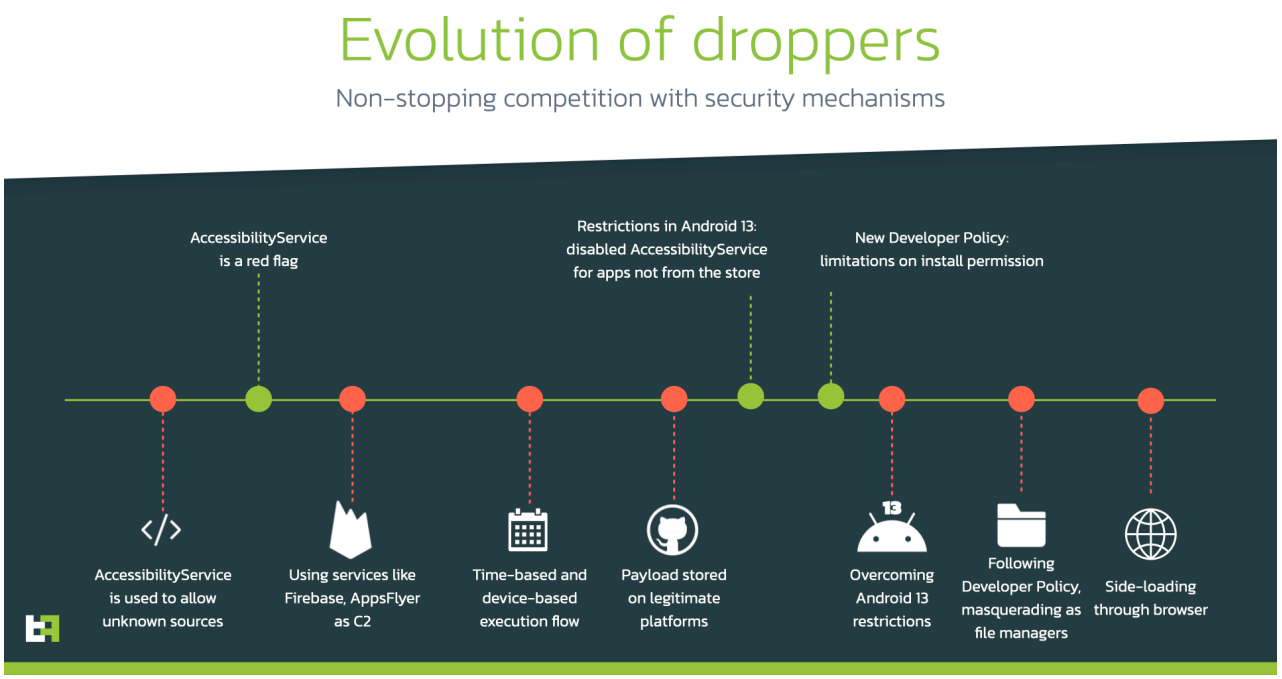
Malware wars: the attack of the droppers

Published: 2024-10-01 · Archived: 2026-04-05 21:17:43 UTC

Another 130.000+ installations of malicious droppers from official store

A year ago, we highlighted a trend of malicious droppers in Google Play store used to distribute banking Trojans. We also predicted further efforts of cybercriminals to reduce the malicious footprint of their malware in order to stay undetected. Distribution through droppers on official stores remains one of the most efficient ways for threat actors to reach a wide and unsuspecting audience. Although other distribution methods are also used depending on cybercriminals targets, resources, and motivation, droppers remain one of the best option on price-efforts-quality ratio, competing with SMiShing.

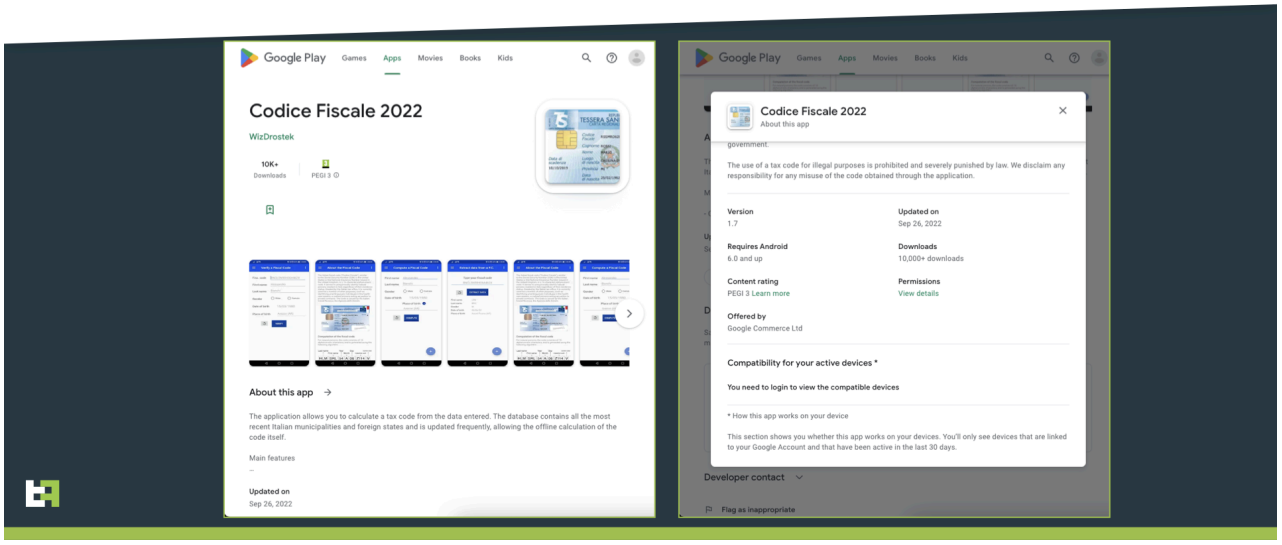
The history of competition between malware authors and security mechanisms knows several twists when new measures are introduced. Droppers on Google Play went from using AccessibilityService to auto-allow installation from unknown sources to using legitimate sources to control them and store malicious payloads. Following the updates to the “Developer Program Policy” and system updates, actors immediately introduce new ways to sneak to the official store, overcoming limitations or adjusting droppers to follow the guidelines and not arouse suspicion. A brief story of that battle is presented on the graph below.



In this blog we uncover additional tactics cybercriminals use in new Google Play droppers discovered by ThreatFabric analysts. These droppers have cumulative number of **130k+** installations distributing Sharkbot and Vultur banking Trojans.

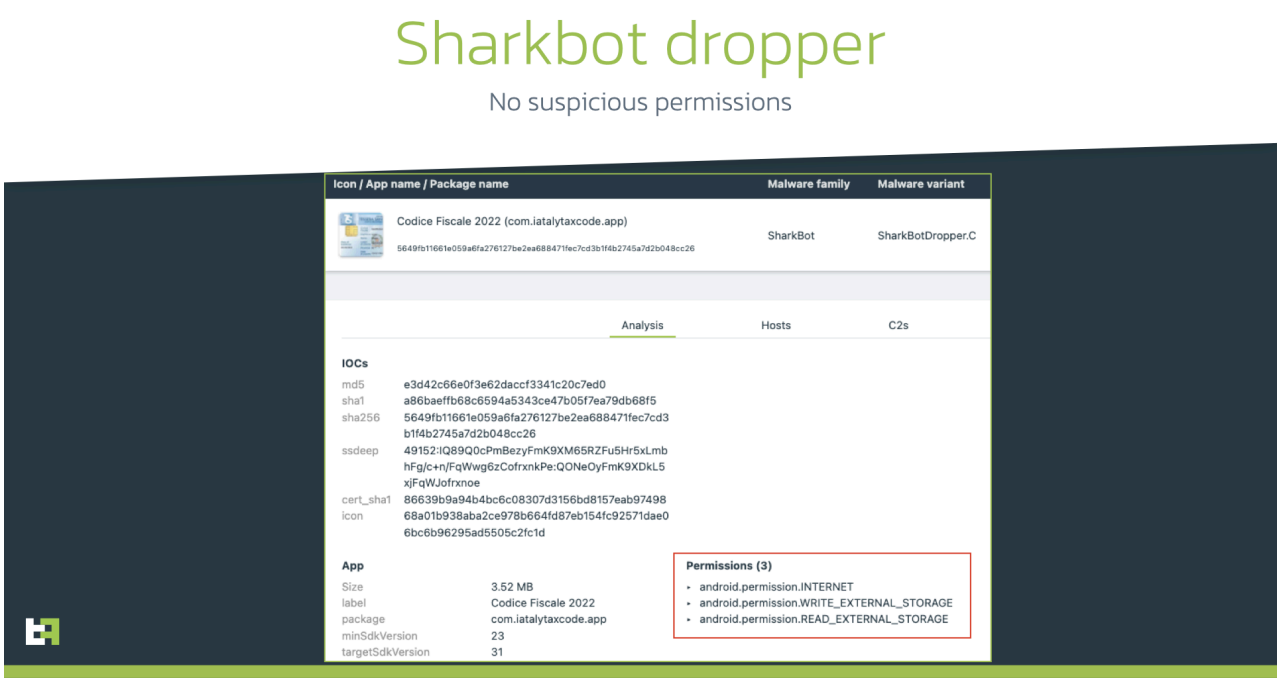
Sharkbot: the less you see, the more they get

In the beginning of October 2022 ThreatFabric analysts spotted a new campaign of banking Trojan Sharkbot, targeting Italian banking users. This campaign involved Sharkbot **version 2.29 – 2.32**. Following the research path, our analysts were able to identify the dropper app located on Google Play with 10k+ installations and disguised as an app to calculate tax code in Italy (“Codice Fiscale”) targeting Italian users.

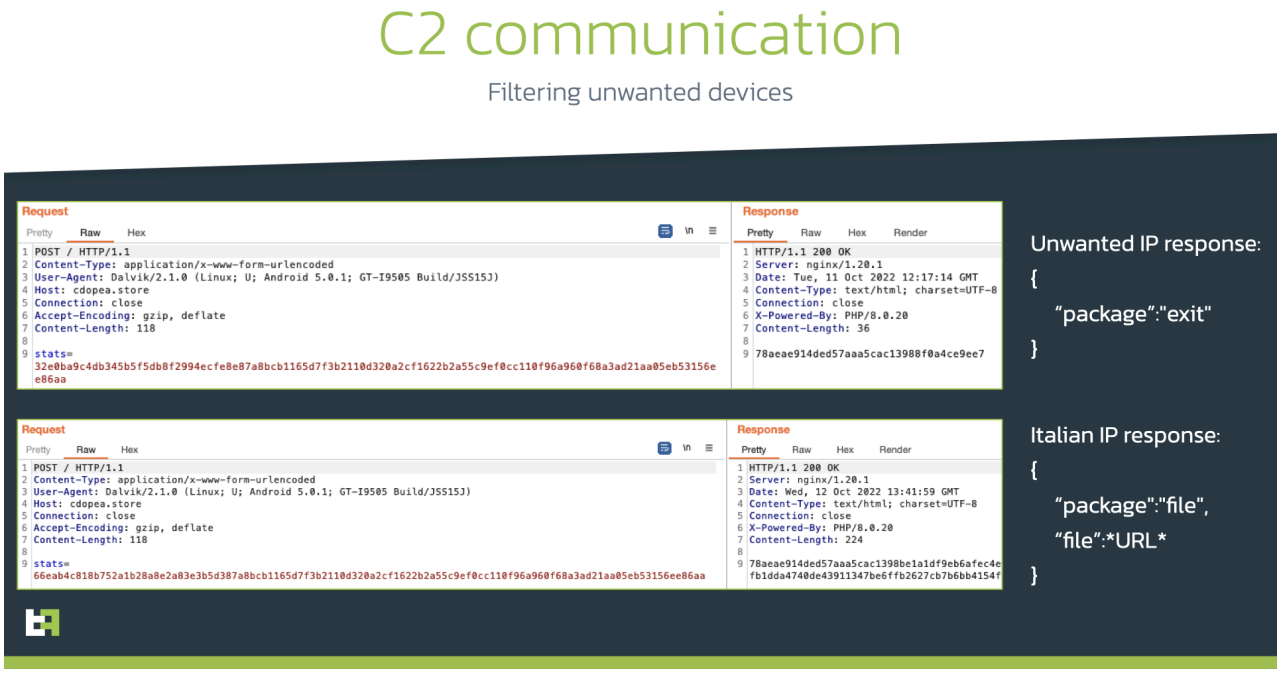


This is not the first time that a Sharkbot dropper sneaks into the official Google store, but this time authors did their best to hide the malicious intents of the dropper. Previous versions of Sharkbot droppers as well as other droppers (including those we highlight below in this blog) include ability to download, install and launch the malicious payload. Obviously, such behaviour is quite suspicious and already made Google to introduce changes to the Developer Program Policy where usage of **REQUEST_INSTALL_PACKAGES** permission was limited to apps that have it as core functionality.

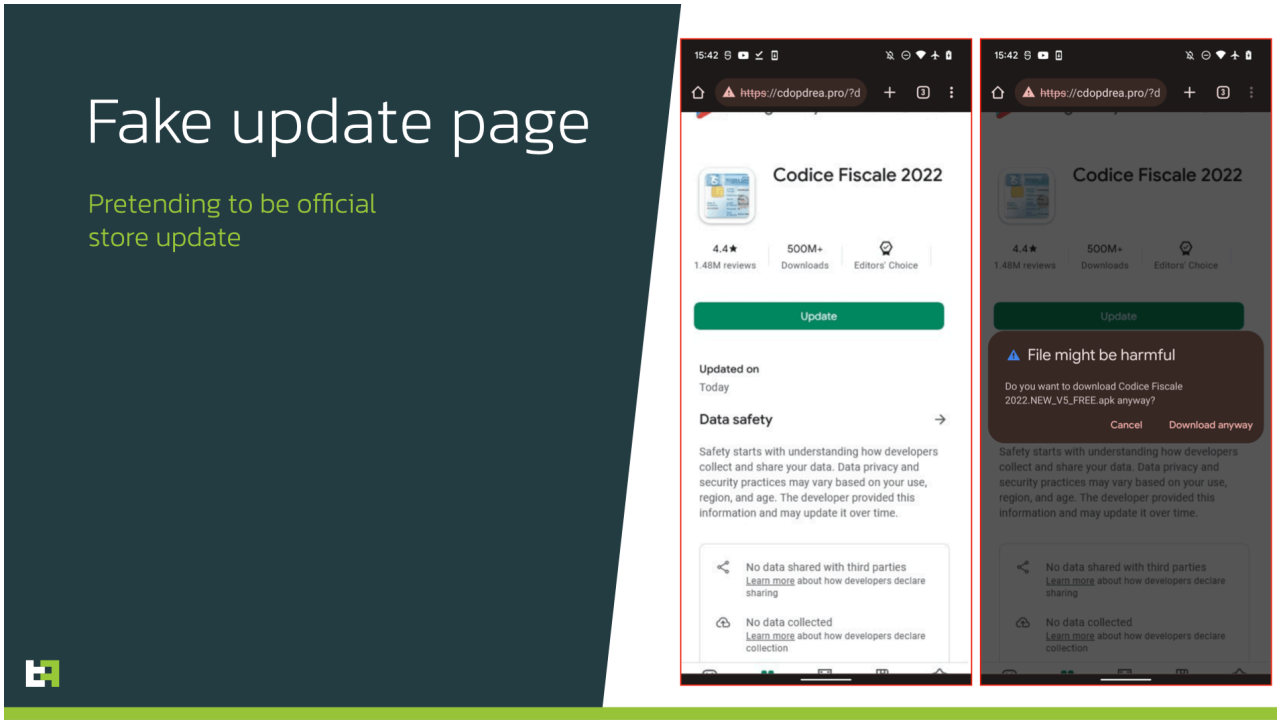
However, in this new iteration, Sharkbot dropper authors tried their best to not include suspicious permissions at all, thus maintaining an extremely low profile. The new dropper has only 3 permissions that are quite common.



To ensure that the dropper is launched on a real targeted device, the app obtains the SIM coutry and compares it to "**it**" (Italy): if not matched, no malicious activity will be performed. Besides, additional checks are made on the C2 side to ensure that the dropper is running on the targeted device: if C2 is reached from a non-Italian IP address, the C2 will respond with a default "exit" message. Otherwise, it will receive a configuration data with the URL containing the payload.

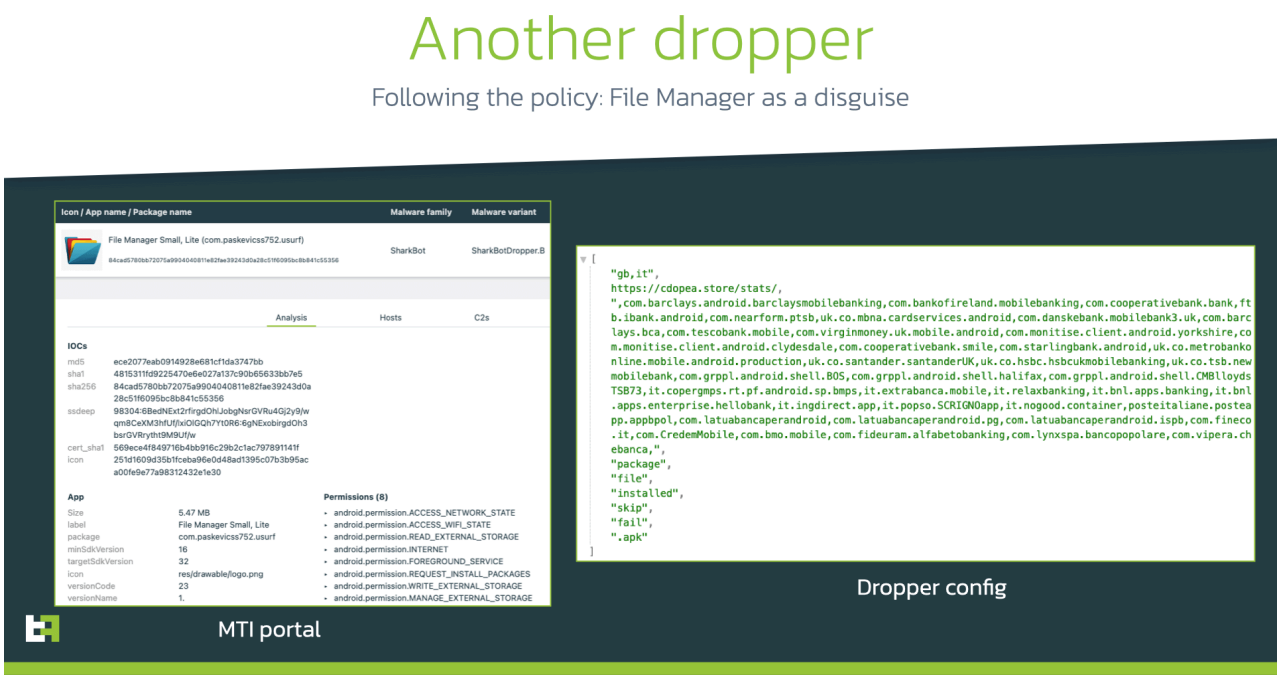


Here the interesting part starts: in order to avoid using REQUEST_INSTALL_PACKAGES permission, the dropper opens a fake Google Play store page impersonating Codice Fiscale app page. It contains fake information about the number of installations and reviews, and urges the victim to perform an update. Shortly after the page is opened, the automatic download starts. Thus, the dropper outsources the download and installation procedure to the browser, avoiding suspicious permissions.



Obviously, such approach requires more actions from the victim, as the browser will show several messages about the downloaded file. However, since victims are sure about the origin of the application, they will highly likely install and run the downloaded Sharkbot payload.

During our investigation, we also found another Sharkbot dropper available on Google Play. It had zero installations at the time of discovery and was quickly removed from the website. The interesting detail about this dropper was that it had the REQUEST_INSTALL_PACKAGES permission in place and operated more in line with usual dropper's behaviour. Actors were also following the updated policy of Google, as this dropper was masqueraded as file manager, a category that is allowed to have this permission due to it being a core functionality.



Similarities in code, C2 communication, and encryption used lead us to the same author behind the older versions of Sharkbot dropper, trying to reduce footprints and stay undetected.

Targets

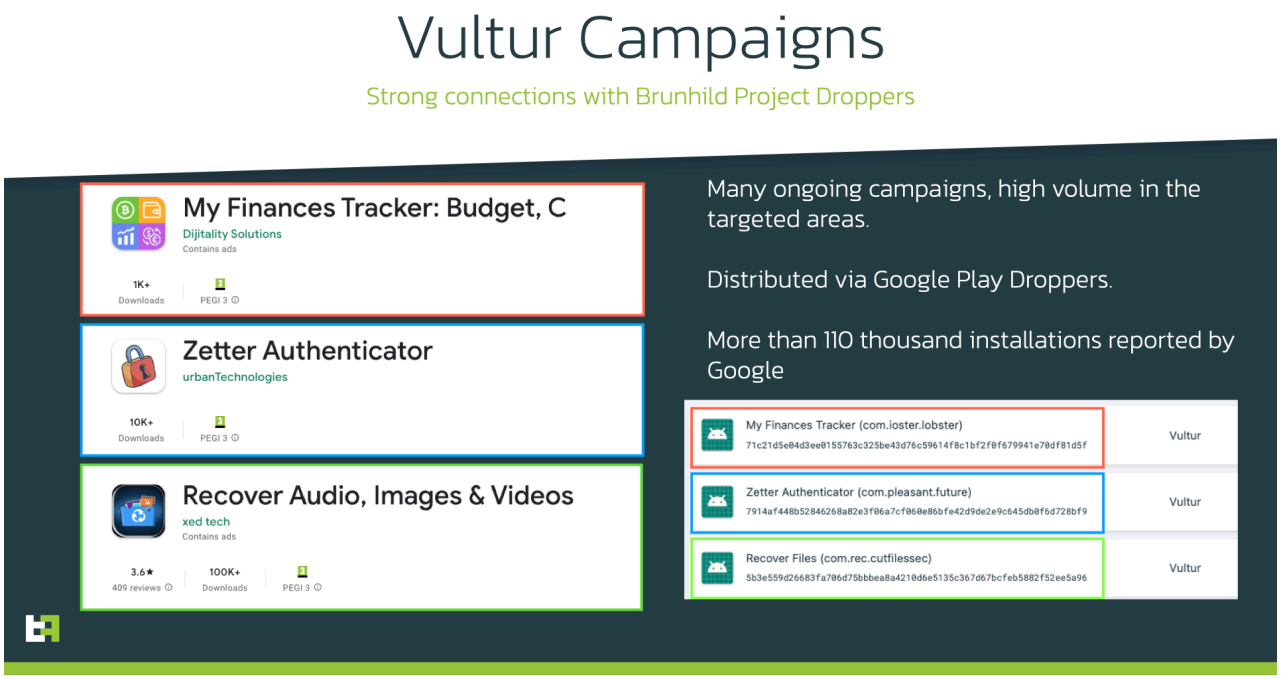
The new "Codice Fiscale" dropper discovered by ThreatFabric is configured to distribute Sharkbot payload to Italian users only, while the other "File Manager" dropper has Italy and UK in its configuration. At the same time, the payload delivered still has banks from Italy, UK, Germany, Spain, Poland, Austria, US, and Australia in its target list. Please, find the full target list in Appendix.

Vultur: Brunhilda is back

Another malware family that has been very active in the last year has been Vultur. First discovered by ThreatFabric in July 2021, Vultur is an Android banking trojan which specializes in stealing PII from infected devices using its screen-streaming capabilities. It is also able to create a remote session on the device using VNC technology to perform actions on the victim's device, effectively leading to On-Device Fraud (ODF).

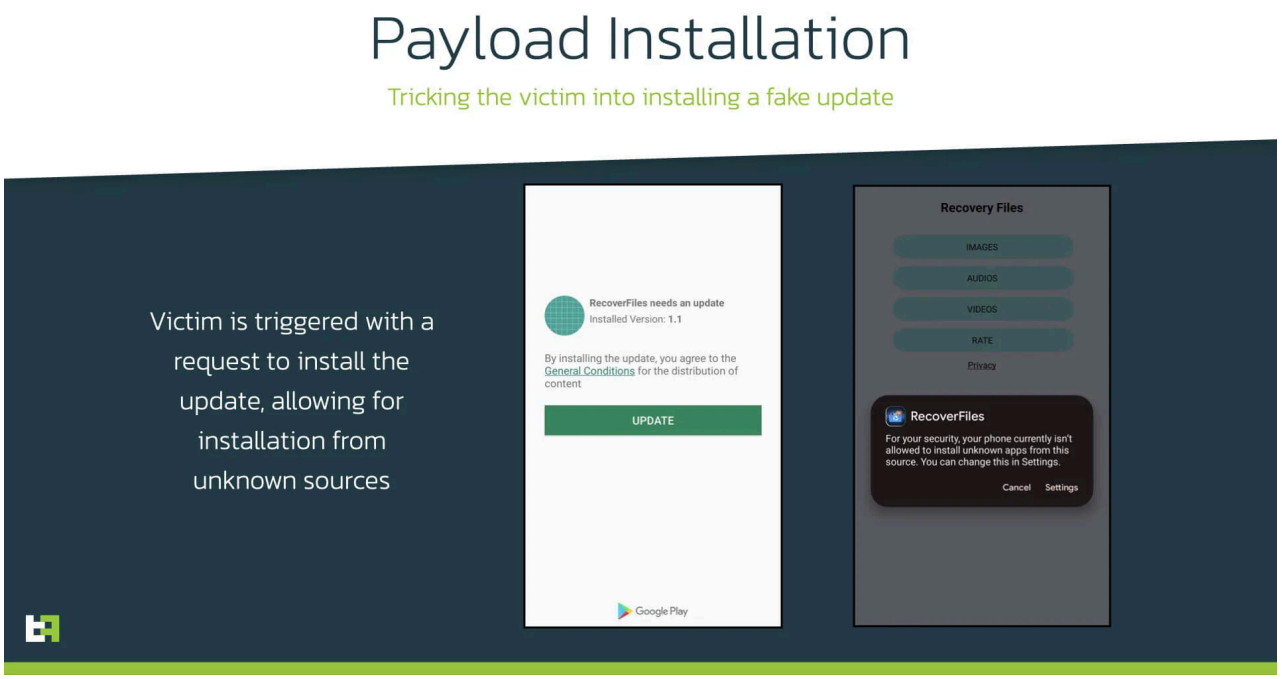
Upon discovery, ThreatFabric first reported the strong connection between this malware family, and the **"Brunhilda Project"** crew. This Threat Actor was known for its central role in the distribution sector of the Android Banking malware landscape thanks to its dropper applications, which managed often to pass Google security checks and be approved on the Google Play Store. Initially, the Brunhilda droppers were deploying a variety of Android malware applications, like for example samples of the malware family Alien. However, after the first discovery of Vultur, every dropper found on the Google Play Store only installed samples belonging to the Vultur malware family.

Recently, ThreatFabric discovered 3 new Droppers on the Google Play store, ranging from 1.000 to 100.000 installations reported by Google. As previous campaigns observed throughout 2022, these droppers pose as applications like security authenticators, or file recovery tools.



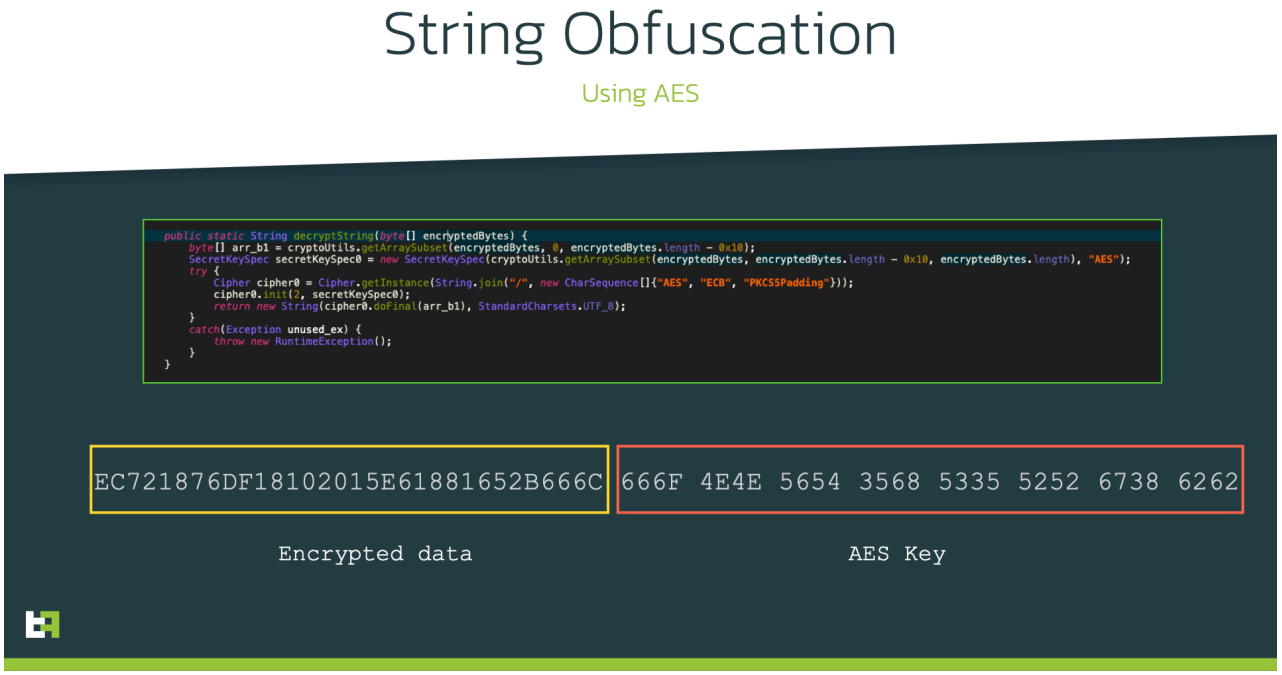
The Dropper

The dropper applications are consistent with the droppers that we reported in our first blog about Vultur, and the modus operandi has not changed much with respect to older variants. As usual, the dropper is made of a trojanized application, which provides the advertised functionality, as well as the hidden dropper functionality. As previously reported, the dropper initially sends a registration message to its C2 server. As a response, the server sends back an appToken, which is then used in the following requests to identify the device. At this point, the dropper prompts the victim with a screen asking to download an **update** for the current application. If the user accepts the displayed request, the dropper proceeds to install Vultur.



In terms of execution of the installation, there are no real updates from previous versions of Brunhilda. However, the dropper currently implements a few obfuscation techniques which were not present in initial versions of the dropper. Firstly, in these new version, the installation logic is not contained in the main DEX file, but in a additional dex file which is loaded dynamically. This additional step can complicate the life of researchers, making it harder to identify the code responsible for malicious activity.

The latest version of Brunhilda also implemented a new layer of obfuscation, which encrypts strings by using AES with a varying key, which is included in the byte array that is given as input to the decryption method, as explained in the picture below:



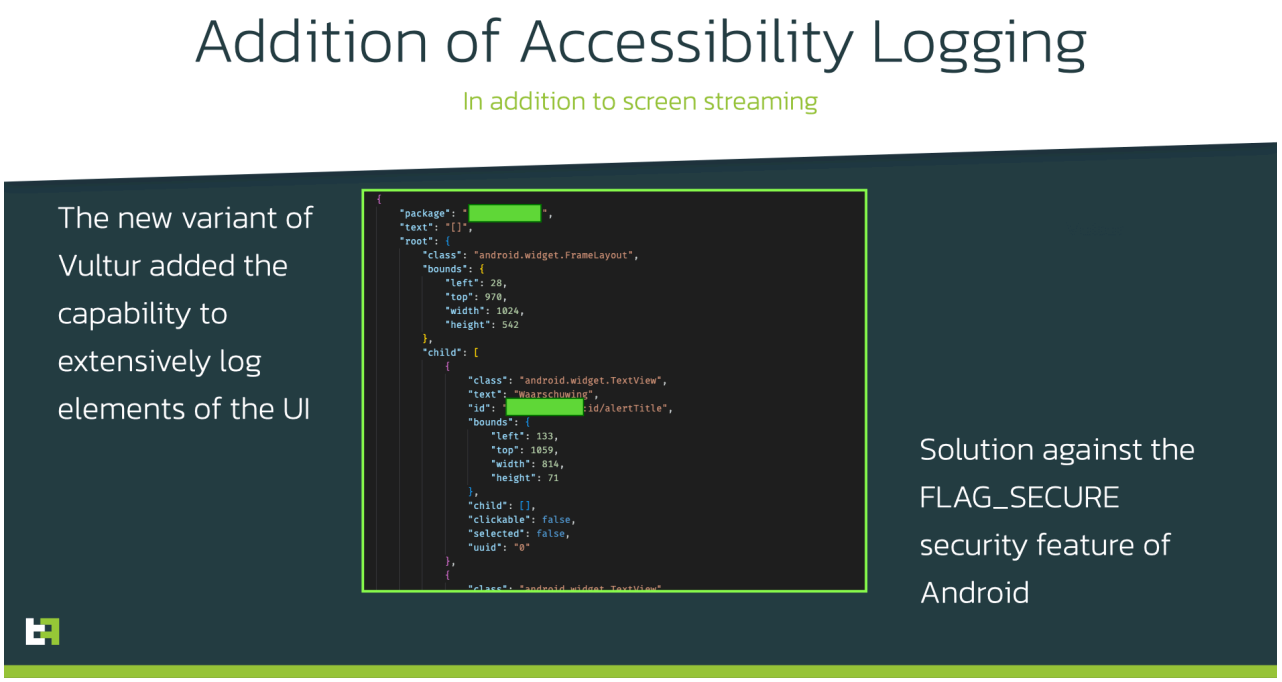
Once the payload is installed, the Brunhilda dropper launches the malware, and then continues existing on the device, acting as the application it is posing as.

Vultur

These Brunhilda droppers all deploy samples belonging to a **novel variant** of Vultur Android Banking malware family.

This new variant maintains the Modus Operandi that characterized the original samples from 2021: once installed, the malware initiates a connection with its C2, and after registering it obtains its configuration containing its targets. Vultur features two separate target lists: one for screen-streaming targets and one for keylogging targets. Similarly to its older variant, the keylogging targets are social and messaging applications, while the screen-streaming targets are applications for online banking and cryptocurrency exchange. However, in this new variant, this second set of targets is also the list of applications for which extensive accessibility logging is performed.

By accessibility logging we mean the extensive logging of all UI elements and all the events associated with them (like for example clicks, gestures, etc). This is not a novel technique, but it is the first time we see it implemented in Vultur. This might be a solution to the issue created by a security flag often used in these banking applications: Android offers a way to tag the content of the window as secure, by using the **“FLAG_SECURE”**, which prevents it “from appearing in screenshots or from being viewed on non-secure displays”. ThreatFabric tested this and is able to confirm that windows with this flag enabled only show a **black screen** during screen-streaming. However, if the **keyboard** is opened during interaction with the secured app, it **will be visible** on the recording as well as all the keys pressed by victim leading to potential theft of input data. In this case, it is possible to obtain enough information to steal credentials even with a black screen, when all the UI events are logged and sent to the C2.



In our previous blog we documented through our research why we believe that Vultur, the malware downladed by these droppers, is a malware family that is not only distributed, but also created by the criminals behind the Brunhilda Project. In addition to the reasons discussed in our previous blog, which focus on the networking protocol used, new variants of Vultur also adopted the very same string obfuscation algorithm discussed in the previous section about the Brunhilda Dropper, further confirming our beliefs about the connection between these two malware families.

Targets

These new Brunhilda-Vultur campaigns have been very active and successful in the last few months, reaching more than 100.000 potential fraud victims. Based on our research and investigation, in addition to cryptowallets which have always been in the target list, the largest campaign we observed focused on UK and Netherlands, while the two smaller and more recent ones switched to Germany, France, and Italy. Full target list of Vultur is provided in Appendix.

Conclusion

Another trend predicted by ThreatFabric's experts comes true and looks like it is here to stay. Malicious dropper applications still find their way to sneak in the official store despite the changes made to the policy and security mechanisms. Distibution through droppers on Google Play still remains the most "affordable" and scalable way of reaching victims for most of the actors of different level. While sophisticated tactics like telephone-oriented attack delivery require more resources and are hard to scale, droppers on official and third-party stores allow threat actors to reach wide unsuspecting audience with reasonable efforts. Such way of distribution of Android banking Trojans is very dangerous as victims may stay unsuspecting for a long time and may not alert their bank about suspicious transactions made without them knowlege. Thus it is very important to take actions on the organisation side to detect such malicous apps and their payloads as well as suspicious behaviour happenning on customer's device.

We at ThreatFabric always report malicous droppers we indentified to remove it from official stores and limit its further distribution. Financial organisations 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 malicous 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, behavioural 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

Sharkbot Droppers

App name	Package name	SHA-256
Codice Fiscale 2022	com.iatalytaxcode.app	5649fb11661e059a6fa276127be2ea688471fec7cd3b1f4b2745a7d2b048cc26
File Manager Small, Lite	com.paskevicss752.usurf	84cad5780bb72075a9904040811e82fae39243d0a28c51f6095bc8b841c55356

Sharkbot Samples

App name	Package name	SHA-256
_Codice Fiscale	com.hzpwksdljgeibc.gmzjwdule	0cbd727b7fa8d9938746475e91fb22a46b75cdcca2778db78073e3c3da70ad31
_Codice Fiscale	com.gxulzkj.atuqczml	008338b39c0abf3aa75e92e845c34ac60e049a480eb1e0ab8d3147085a7bb745

Brunhilda Droppers

App name	Package name	SHA-256
My Finances Tracker	com.all.finance.plus	0626e98f9988c63684e575d7a0df839240f7963aed38f82010e63b1b85a9ef61
RecoverFiles	com.umac.recoverallfilepro	e94a6f7dcdddd4b8c18110993f118f86d3cbfe1faf330f9968aaa7095dd189a4
Zetter Authenticator	com.zetter.fastchecking	54139e2e008ed2ebcb4fc71d8aa2470727a724c8607464d9c3688e9506952529

Vultur Samples

App name	Package name	SHA-256
RecoverFiles	com.accessible.recoverypro	cae3a48013fcea931f6b84e196f625e27017a1cdc97c1d86c8077db431abd508

App name	Package name	SHA-256
Zetter Authenticator	com.zforce.setupex	8584d43067535dc97d12c4565e1636e3a1963421fe811ff6e58b4dbd7e5b947d

Sharkbot Targets

Package name	App name
au.com.nab.mobile	NAB Mobile Banking
at.erstebank.george	George Österreich
com.grppl.android.shell.BOS	Bank of Scotland Mobile Banking: secure on the go
de.number26.android	N26 — The Mobile Bank
co.bitx.android.wallet	Luno: Buy Bitcoin, Ethereum and Cryptocurrency
com.fineco.it	Fineco
com.paypal.android.p2pmobile	PayPal Mobile Cash: Send and Request Money Fast
es.lacaixa.mobile.android.newwapicon	CaixaBank
com.targo_prod.bad	TARGOBANK Mobile Banking
com.grppl.android.shell.halifax	Halifax: the banking app that gives you extra
pl.pkobp.iko	IKO
org.stgeorge.bank	St.George Mobile Banking
it.bnl.apps.banking	BNL
com.vipera.chebanca	CheBanca!
uk.co.santander.santanderUK	Santander Mobile Banking
com.wf.wellsfargomobile	Wells Fargo Mobile
com.starfinanz.smob.android.*	Sparkasse
piuk.blockchain.android	Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum
com.commbank.netbank	CommBank
es.unicajabanco.app	Unicaja Banco
uk.co.mbna.cardservices.android	MBNA - Card Services App
de.postbank.finanzassistent	Postbank Finanzassistent
com.barclays.android.barclaysmobilebanking	Barclays
com.konylabs.capitalone	Capital One® Mobile

Package name	App name
com.advanzia.mobile	Advanzia
uk.co.tsb.newmobilebank	TSB Mobile Banking
com.latuabancaperandroid	Intesa Sanpaolo Mobile
com.citi.citimobile	Citi Mobile®
com.virginmoney.uk.mobile.android	Virgin Money Mobile Banking
com.grppl.android.shell.CMBlloydsTSB73	Lloyds Bank Mobile Banking: by your side
posteitaliane.posteapp.appbpol	BancoPosta
com.lynxspa.bancopopolare	YouApp
de.commerzbanking.mobil	Commerzbank Banking - The app at your side
uk.co.hsbc.hsbcukmobilebanking	HSBC UK Mobile Banking
com.CredemMobile	Credem
com.starlingbank.android	Starling Bank - Better Mobile Banking
com.binance.dev	Binance - Buy & Sell Bitcoin Securely
com.cooperativebank.bank	The Co-operative Bank
com.transferwise.android	TransferWise Money Transfer
com.usbank.mobilebanking	U.S. Bank - Inspired by customers

Vultur Targets

Package name	Application name
asia.coins.mobile	Coins.ph Wallet
be.aion.android.app	Aion Bank
btc.org.freewallet.app	Bitcoin Wallet. Buy & Exchange BTC coin – Freewallet
bvm.bvmapp	Knab Bankieren
cash.klever.blockchain.wallet	Klever Wallet: Buy Bitcoin, Ethereum, Tron, Crypto
cedacri.mobile.bank.crbolzano	isi-mobile Cassa di Risparmio
cedacri.mobile.bank.esperia	Mediobanca Private Banking
co.bitx.android.wallet	Luno: Buy Bitcoin, Ethereum and Cryptocurrency
co.clabs.valora	Valora - Crypto Wallet
co.edgesecure.app	Edge - Bitcoin, Ethereum, Monero, Ripple Wallet

Package name	Application name
co.mona.android	Crypto.com - Buy Bitcoin Now
co.uk.Nationwide.Mobile	Nationwide Banking App
com.CredemMobile	Credem
com.IngDirectAndroid	ING France
com.VBSmartPhoneApp	BankUp Mobile
com.abnamro.nl.mobile.payments	ABN AMRO Mobiel Bankieren
com.americanexpress.android.acctsvcs.it	Amex Italia
com.americanexpress.android.acctsvcs.uk	Amex United Kingdom
com.arkea.android.application.cmb	Crédit Mutuel de Bretagne
com.bankid.bus	BankID säkerhetsapp
com.banknorwegian	Bank Norwegian
com.barclays.android.barclaysmobilebanking	Barclays
com.barclays.bca	Barclaycard
com.bbva.italy	BBVA Italia Banca Online
com.binance.dev	Binance - Buy & Sell Bitcoin Securely
com.bitcoin.mwallet	Bitcoin Wallet
com.bitfinex.mobileapp	Bitfinex
com.bitpanda.bitpanda	Bitpanda - Buy Bitcoin in minutes
com.bittrex.trade	Bittrex Global
com.bituniverse.portfolio	BitUniverse:Crypto Trading Bot
com.boursorama.android.clients	Boursorama Banque
com.breadwallet	BRD Bitcoin Wallet. Buy BTC Bitcoin Cash, Ethereum
com.bunq.android	bunq - bank of The Free
com.bybit.app	Bybit: Crypto Trading Exchange
com.caisseepargne.android.mobilebanking	Banque
com.cic_prod.bad	CIC
com.cm_prod.bad	Crédit Mutuel
com.coinbase.android	Coinbase – Buy & Sell Bitcoin. Crypto Wallet

Package name	Application name
com.coinbase.pro	Coinbase Pro – Bitcoin & Crypto Trading
com.coinbase.wallite	Coinbase Wallet Lite
com.coinomi.wallet	Coinomi Wallet :: Bitcoin Ethereum Altcoins Tokens
com.coinspot.app	CoinSpot - Buy & Sell Bitcoin
com.comeco.teo	TEO - Das neue Multibanking
com.cooperativebank.bank	The Co-operative Bank
com.crypterium	Crypterium Bitcoin Wallet
com.crypto.multiwallet	Guarda Crypto Bitcoin Wallet
com.cryptonator.android	Cryptonator cryptocurrency wallet
com.db.pbc.miabanca	La Mia Banca
com.db.pwcc.dbmobile	Deutsche Bank Mobile
com.defi.wallet	Crypto.com l DeFi Wallet
com.digifinex.app	DigiFinex - Buy & Sell Bitcoin, Crypto Trading
com.enjin.mobile.wallet	Enjin: Bitcoin, Ethereum, Blockchain Crypto Wallet
com.etoro.openbook	eToro - Smart Crypto Trading Made Easy
com.etoro.wallet	eToro Money
com.fideuram.alfabetobanking	Alfabeto Banking
com.fidor.fsw	Fidor Smart Banking
com.fineco.it	Fineco
com.firstdirect.bankingonthego	first direct
com.gemini.android.app	Gemini: Buy Bitcoin Instantly
com.getpenta.app	Penta – Business Banking App
com.grppl.android.shell.BOS	Bank of Scotland Mobile Banking: secure on the go
com.grppl.android.shell.CMBlloydsTSB73	Lloyds Bank Mobile Banking: by your side
com.grppl.android.shell.halifax	Halifax: the banking app that gives you extra
com.hanseaticbank.banking	Hanseatic Bank Mobile
com.hittechsexpertlimited.hitbtc	HitBTC – Bitcoin Trading and Crypto Exchange
com.ie.capitalone.uk	Capital One UK

Package name	Application name
com.ing.mobile	ING Bankieren
com.kontist	Kontist Tax Service
com.kraken.invest.app	Kraken - Buy Bitcoin & Crypto
com.kraken.trade	Pro: Advanced Bitcoin & Crypto Trading
com.krakenfutures	Kraken Futures: Bitcoin & Crypto Futures Trading
com.kubi.kucoin	KuCoin: Bitcoin Exchange & Crypto Wallet
com.latuabancaperandroid	Intesa Sanpaolo Mobile
com.latuabancaperandroid.pg	Intesa Sanpaolo Business
com.liberty.jaxx	Jaxx Liberty: Blockchain Wallet
com.lumiwallet.android	Lumi Crypto and Bitcoin Wallet
com.lynxspa.bancopopolare	YouApp
com.mediolanum.android.fullbanca	Mediolanum
com.mercuryo.app	Mercuryo Bitcoin Cryptowallet
com.mycelium.wallet	Mycelium Bitcoin Wallet
com.ocito.cdn.activity.banquesmc	SMC pour Mobile
com.ocito.cdn.activity.creditdunord	Crédit du Nord pour Mobile
com.okinc.okex.gp	OKEx - Bitcoin/Crypto Trading Platform
com.opentecheng.android.webank	Webank
com.orangebank.android	Orange Bank
com.paxful.wallet	Paxful Bitcoin Wallet
com.paysend.app	Money Transfer App Paysend
com.phemex.app	Phemex: Buy Crypto & Bitcoin
com.pionex.client	Pionex - Crypto Trading Bot
com.plunien.poloniex	Poloniex Crypto Exchange
com.plutus.wallet	Abra: Bitcoin, XRP, LTC
com.rbs.mobile.android.natwest	NatWest Mobile Banking
com.rbs.mobile.android.rbs	Royal Bank of Scotland Mobile Banking
com.rbs.mobile.android.ubn	Ulster Bank NI Mobile Banking

Package name	Application name
com.revolut.revolut	Revolut - Get more from your money
com.robinhood.android	Robinhood - Investment & Trading, Commission-free
com.satispay.customer	Satispay
com.scrignosa	SCRIGNOIdentiTel
com.sella.BancaSella	Banca Sella
com.sisal.sisalpay	Mooney App: pagamenti digitali
com.squareup.cash	Cash App
com.starfinanz.smob.android.bwmobilbanking	BW-Mobilbanking mit Smartphone und Tablet
com.starfinanz.smob.android.sfinanzstatus	Sparkasse Ihre mobile Filiale
com.starlingbank.android	Starling Bank - Better Mobile Banking
com.stoegerit.outbank.android	Outbank - 360° Banking
com.stormgain.mobile	StormGain: Bitcoin Wallet & Crypto Exchange App
com.superchain.lbankgoogle	LBank - Buy Bitcoin & Crypto
com.tabtrader.android	TabTrader Buy Bitcoin and Ethereum on exchanges
com.targo_prod.bad	TARGOBANK Mobile Banking
com.tescobank.mobile	Tesco Bank Mobile Banking
com.transferwise.android	TransferWise Money Transfer
com.triodos.bankingnl	Triodos Bankieren NL
com.unicredit	Mobile Banking UniCredit
com.uphold.wallet	Uphold - Trade, Invest, Send Money For Zero Fees
com.vipera.chebanca	CheBanca!
com.virginmoney.uk.mobile.android	Virgin Money Mobile Banking
com.wallet.crypto.trustapp	Trust: Crypto & Bitcoin Wallet
com.youhodler.youhodler	YouHodler - Crypto and Bitcoin Wallet
com.zengo.wallet	ZenGo Crypto & Bitcoin Wallet: Buy, Earn & Trade
de.bbbank.banking.privat	BBBank-Banking classic
de.bs.ibanking	OLB Banking
de.comdirect.app	comdirect

Package name	Application name
de.commerzbanking.mobil	Commerzbank Banking - The app at your side
de.fiducia.smartphone.android.banking.vr	VR Banking Classic
de.fiduciagad.banking.vr	VR Banking - einfach sicher
de.ingdiba.bankingapp	ING Banking to go
de.number26.android	N26 — The Mobile Bank
de.postbank.bestsign	Postbank BestSign
de.postbank.finanzassistent	Postbank Finanzassistent
de.psd.banking.app	PSD Banking
de.psd.banking.privat	PSD Banking Classic
de.santander.presentation	Santander Banking
de.schildbach.wallet	Bitcoin Wallet
de.sdvrz.ihb.mobile.secureapp.sparda.produktion	SpardaSecureApp
de.sparda.banking.privat	SpardaBanking+
de.spardab.banking.privat	Sparda Berlin
eth.org.freewallet.app	Ethereum Wallet. Buy & Exchange ETH — Freewallet
eu.qonto.qonto	Qonto • Easy Business Banking
eu.unicreditgroup.hvbapptan	HVB Mobile Banking
exodusmovement.exodus	Exodus: Crypto Bitcoin Wallet
fr.bnpp.digitalbanking	Hello bank! par BNP Paribas
fr.creditagricole.androidapp	Ma Banque
fr.hsbc.hsbcfrance	HSBC France
fr.lcl.android.customerarea	Mes Comptes - LCL
fr.mafrenchbank	Ma French Bank
io.atomicwallet	Bitcoin Wallet & Ethereum Ripple ZIL DOT
io.bluewallet.bluewallet	BlueWallet Bitcoin Wallet
io.cex.app.prod	CEX.IO Cryptocurrency Exchange
io.metamask	MetaMask - Buy, Send and Swap Crypto
io.safepal.wallet	SafePal-Crypto wallet BTC NFTs

Package name	Application name
it.bcc.iccrea.mycartabcc	myCartaBCC
it.bnl.apps.banking	BNL
it.bnl.apps.banking.privatebnl	My Private Banking
it.bper.mobile.mymoney	Smart My Money
it.caitalia.apphub	Crédit Agricole Italia
it.carige	Carige Mobile
it.cedacri.hb2.bpbari	Mi@
it.cedacri.hb3.desio.brianza	D-Mobile
it.copergmps.rt.pf.android.sp.bmps	Banca MPS
it.creval.bancaperta	Bancaperta
it.gruppobper.ams.android.bper	Smart Mobile Banking
it.gruppobper.smartbpercard	Smart BPER Card
it.gruppocariparma.nowbanking	Nowbanking
it.hype.app	Hype
it.icbpi.mobile	Nexi Pay
it.ingdirect.app	ING Italia
it.nogood.container	UBI Banca
it.phoenixspa.inbank	Inbank
it.popso.SCRIGNOapp	SCRIGNOapp
it.relaxbanking	RelaxBanking Mobile
mobi.societegenerale.mobile.lappli	L’Appli Société Générale
mobi.societegenerale.mobile.lapplipro	L’Appli Pro Société Générale
mw.org.freewallet.app	Bitcoin & Crypto Blockchain Wallet: Freewallet
net.bitstamp.app	Bitstamp – Buy & Sell Bitcoin at Crypto Exchange
net.bnpparibas.mescomptes	Mes Comptes BNP Paribas
net.safemoon.androidwallet	SafeMoon
nl.asnbank.asnbankieren	ASN Mobiel Bankieren
nl.rabomobiel	Rabo Bankieren

Package name	Application name
nl.regiobank.regiobankieren	RegioBank - Mobiel Bankieren
nl.snsbank.snsbankieren	SNS Mobiel Bankieren
one.tomorrow.app	Tomorrow: Mobile Banking
org.electrum.electrum	Electrum Bitcoin Wallet
org.toshi	Coinbase Wallet — Crypto Wallet & DApp Browser
piuk.blockchain.android	Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum
posteitaliane.posteapp.appbpol	BancoPosta
se.bankgirot.swish	Swish payments
uk.co.hsbc.hsbcukmobilebanking	HSBC UK Mobile Banking
uk.co.mbna.cardservices.android	MBNA - Card Services App
uk.co.metrobankonline.mobile.android.production	Metro Bank
uk.co.santander.santanderUK	Santander Mobile Banking
uk.co.tsb.newmobilebank	TSB Mobile Banking

Source: https://www.threatfabric.com/blogs/the-attack-of-the-droppers.html