Vultur, with a V for VNC

Published: 2024-10-01 · Archived: 2026-04-06 00:17:39 UTC

Introduction

In late March 2021, ThreatFabric detected a new RAT malware that we dubbed Vultur due to its full visibility on victims device via VNC. For the first time we are seeing an Android banking trojan that has screen recording and keylogging as main strategy to harvest login credentials in an automated and scalable way. The actors chose to steer away from the common HTML overlay strategy we usually see in other Android banking Trojans: this approach usually requires more time and effort from the actors in order to steal relevant information from the user. Instead, they chose to simply record what is shown on the screen, effectively obtaining the same end result.

Based on the intelligence gathered, ThreatFabric was able to obtain the list of apps targeted by Vultur. Italy, Australia and Spain were the countries with most banking institutions targeted. In addition, many crypto-wallets are targeted, which is in line with the trend we observed in our previous blog "The Rage of Android Banking Trojans".

During the investigation ThreatFabric analysts discovered its connection with a well-known dropper framework called Brunhilda, which uses droppers located in Google Play to distribute malware (MITRE T1475).

In this blogpost ThreatFabric will prove that this dropper and Vultur are both developed by the same threat actor group. The choice of developing its own private trojan, instead of renting third-party malware, displays a strong motivation from this group, paired with the overall high level of structure and organization present in the bot as well as the server code.

NOTE : **ThreatFabric wants to make clear that both AlphaVNC and ngrok (the third party softwares on which Vultur relies on to operate) are legitimate and legal products. The developers that created these projects have no control over the misuse of their software.**

Context

In September 2020, Bitdefender published a Bitdefender report about malware droppers found on Google Play. The report states that these droppers were used to distribute Cerberus banking malware. However, we believe that it was in fact Alien banking malware, the successor of Cerberus, first reported by ThreatFabric in September 2020.

If the user pays attention to the notification panel, he would also be able to see that Vultur, in this case masquerading as an app called "Protection Guard", is projecting the screen.

Communication

C2 Methods

Below is a complete list of the methods supported by the bot. These are the commands that the bot can send to the C2 to request, or to send back, information:

Method	Description
vnc.register	Sends registration information
vnc.status	Sends device status (is DeviceAdmin, is AccessibilityService enabled, is display on) and VNC address

Method	Description
vnc.apps	Sends the list of installed packages
vnc.keylog	Sends pressed keys log
vnc.syslog	Sends logs
crash.logs	Sends crash logs (logs all the content on the screen via accessibility logging)

FCM Commands

Below is a complete list of the commands that the bot can receive via FirebaseCloudMessaging:

Method	Description
registered	Received after successful registration
start	Starts VNC connection using ngrok
stop	Stops VNC connection by deleting address, killing the ngrok process and stopping VNC service
unlock	Unlocks screen
delete	Uninstalls bot package
pattern	Provides a pattern of gesture/stroke to be executed on the device

C2 paths

These are the endpoints reachable on the C2:

Path	Description
/rpc/	Endpoint for C2 communication via JSON-RPC
/upload/	Endpoint for uploading files via POST (e.g. screen record)
/version/app/?filename=ngrok&arch={arm|386}	Endpoint for downloading the corresponding ngrok version

Targets

Vultur contains two sets of targets: screen recording and keylogging. The first list reported in the appendix includes all the applications that will be victim of screen recording using AlphaVNC, while the second list includes all the applications targeted by the keylogging feature. The following chart shows the number of targeted banking applications per country (applications of cryptocurrency wallets and social applications are shown separately):

Conclusion

The story of Vultur shows again how actors shift from using rented Trojans (MaaS) that are sold on underground markets towards proprietary/private malware tailored to the needs of the actor. It enables us to observe a group that covers both processes of distribution and operation of malicious software.

Banking threats on the mobile platform are no longer only based on well-known overlay attacks, but are evolving into RAT-like malware, inheriting useful tricks like detecting foreground applications to start screen recording. This brings the threat

to another level, as such features open the door for on-device fraud, circumventing detection based on phishing MO's that require fraud to be performed from a new device: With Vultur fraud can happen on the infected device of the victim. These attacks are scalable and automated since the actions to perform fraud can be scripted on the malware backend and sent in the form of sequenced commands.

As the mobile channels of financial institutions continue to grow, mobile banking malware will only become more popular. Besides a steep increase in mobile malware volumes targeting banking apps last and this year, we see mobile malware becoming more and more sophisticated enabling hard-to-detect large scale attacks. This means that financial institutions should consider preparing themselves by better understanding the risk posed to their mobile-first strategy based on the current mobile threat landscape.

CSD & MTI

ThreatFabric makes it easier than it has ever been to run a secure mobile payments business. With the most advanced threat intelligence for mobile banking, financial institutions are able to build a threat-driven mobile security strategy and use this unique knowledge to detect financial fraud on the mobile devices of their customers in real-time.

Together with our customers and partners, we are building an easy-to-access information system where financial institutions have more visibility on their mobile banking threats in order to protect their end customers.

You can request our free trial for our MTI feed for the following TIPs:

- Anomali
- ThreatConnect
- ThreatQuotient

If you want more information on how our MTI and CSD solutions can help your organization, feel free to contact us at: sales@threatfabric.com

Appendix

Brunhilda Dropper

App name	Package name	SHA-256
Protection Guard	com.protectionguard.app	d3dc4e22611ed20d700b6dd292ffddbc595c42453f18879f2ae4693a4d4d925a

Vultur

App name	Package name	SHA-256
Protection Guard	com.appsmastersafey	f4d7e9ec4eda034c29b8d73d479084658858f56e67909c2ffedf9223d7ca9bd
Authenticator 2FA	com.datasafeaccountsanddata.club	7ca6989ccfb0ad0571aef7b263125410a5037976f41e17ee7c022097f827bd7

Screen recording targets

Package Name	Application Label
com.commbank.netbank	CommBank
au.com.nab.mobile	NAB Mobile Banking
org.westpac.bank	Westpac Mobile Banking
au.com.macquarie.banking	Macquarie Mobile Banking
com.bendigobank.mobile	Bendigo Bank
au.com.suncorp.SuncorpBank	Suncorp Bank
au.com.ingdirect.android	ING Australia Banking
com.anz.android.gomoney	ANZ Australia
com.abnamro.nl.mobile.payment	ABN AMRO Wallet App
com.ing.mobile	ING Bankieren
it.ingdirect.app	ING Italia
posteitaliane.posteapp.appposteid	PosteID
posteitaliane.posteapp.apppostepay	Postepay
com.bankofqueensland.boq	BOQ Mobile
au.com.amp.myportfolio.android	My AMP
au.com.bankwest.mobile	Bankwest
au.com.mebank.banking	ME Bank
com.fusion.banking	Bank Australia app
org.bom.bank	Bank of Melbourne Mobile Banking
org.stgeorge.bank	St.George Mobile Banking
au.com.cua.mb	CUA Mobile Banking
au.com.hsbc.hsbcaustralia	HSBC Australia
com.virginmoney.cards	Virgin Money Credit Card
org.banksa.bank	BankSA Mobile Banking
cedacri.mobile.bank.crbolzano	isi-mobile Cassa di Risparmio
com.latuabancaperandroid.pg	Intesa Sanpaolo Business
cedacri.mobile.bank.esperia	Mediobanca Private Banking
com.ria.moneytransfer	Ria Money Transfer – Send Money Online Anywhere
it.bnl.apps.banking.privatebnl	My Private Banking
it.bcc.iccrea.mycartabcc	myCartaBCC

Package Name	Application Label
it.cedacri.hb3.desio.brianza	D-Mobile
it.cedacri.hb2.bpbari	Mi@
it.relaxbanking	RelaxBanking Mobile
com.sella.BancaSella	Banca Sella
it.caitalia.apphub	Crédit Agricole Italia
com.unicredit	Mobile Banking UniCredit
com.latuabancaperandroid	Intesa Sanpaolo Mobile
posteitaliane.posteapp.appbpol	BancoPosta
it.copergmps.rt.pf.android.sp.bmps	Banca MPS
com.lynxspa.bancopopolare	YouApp
it.nogood.container	UBI Banca
it.gruppobper.ams.android.bper	Smart Mobile Banking
it.gruppobper.smartbpercard	Smart BPER Card
it.bper.mobile.mymoney	Smart Mobile My Money
com.vipera.chebanca	CheBanca!
com.CredemMobile	Credem
com.opentecheng.android.webank	Webank
com.mediolanum.android.fullbanca	Mediolanum
it.popso.SCRIGNOapp	SCRIGNOapp
it.icbpi.mobile	Nexi Pay
com.scrignosa	SCRIGNOIdentiTel
com.VBSmartPhoneApp	BankUp Mobile
it.carige	Carige Mobile
it.creval.bancaperta	Bancaperta
it.bnl.apps.banking	BNL
it.volksbank.android	Volksbank · Banca Popolare
es.bancosantander.apps	Santander
net.inverline.bancosabadell.officelocator.android	Banco Sabadell App. Your mobile bank
es.liberbank.cajasturapp	Banca Digital Liberbank
es.lacaixa.mobile.android.newwapicon	CaixaBank

Package Name	Application Label
com.bankinter.launcher	Bankinter Móvil
com.bbva.bbvacontigo	BBVA Spain
es.cecabank.ealia2103appstore	UniPay Unicaja
com.db.pbc.mibanco	Mi Banco db
com.grupocajamar.wefferent	Grupo Cajamar
es.univia.unicajamovil	UnicajaMovil
es.bancosantander.empresas	Santander Empresas
com.rsi	ruralvía
app.wizink.es	WiZink, tu banco senZillo
es.cm.android	Bankia
com.imaginbank.apps	Imagin. Much more than an app to manage your money
es.ibercaja.ibercajaapp	Ibercaja
com.bendigobank.mobile	Bendigo Bank
com.mfoundry.mb.android.mb	Multiple minor US financial institution
com.popular.android.mibanco	Mi Banco Mobile
com.grupocajamar.wefferent	Grupo Cajamar
es.unicajabanco.app	Unicaja Banco
es.univia.unicajamovil	UnicajaMovil
com.binance.dev	Binance - Buy & Sell Bitcoin Securely
com.coinbase.android	Coinbase – Buy & Sell Bitcoin. Crypto Wallet
com.coinbase.pro	Coinbase Pro – Bitcoin & Crypto Trading
com.coinbase.wallite	Coinbase Wallet Lite
org.toshi	Coinbase Wallet — Crypto Wallet & DApp Browser
com.defi.wallet	Crypto.com l DeFi Wallet
co.mona.android	Crypto.com - Buy Bitcoin Now
piuk.blockchain.android	Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum
com.wallet.crypto.trustapp	Trust: Crypto & Bitcoin Wallet
exodusmovement.exodus	Exodus: Crypto Bitcoin Wallet
io.atomicwallet	Bitcoin Wallet & Ethereum Ripple ZIL DOT
com.coinomi.wallet	Coinomi Wallet :: Bitcoin Ethereum Altcoins Tokens

Package Name	Application Label
com.krakenfutures	Kraken Futures: Bitcoin & Crypto Futures Trading
com.kraken.trade	Pro: Advanced Bitcoin & Crypto Trading
com.kraken.invest.app	Kraken - Buy Bitcoin & Crypto
io.cex.app.prod	CEX.IO Cryptocurrency Exchange
net.bitstamp.app	Bitstamp – Buy & Sell Bitcoin at Crypto Exchange
com.etoro.wallet	eToro Money
com.kubi.kucoin	KuCoin: Bitcoin Exchange & Crypto Wallet
com.bittrex.trade	Bittrex Global
com.bitfinex.mobileapp	Bitfinex
com.plunien.poloniex	Poloniex Crypto Exchange
com.hittechsexpertlimited.hitbtc	HitBTC – Bitcoin Trading and Crypto Exchange
com.paxful.wallet	Paxful Bitcoin Wallet
com.cryptonator.android	Cryptonator cryptocurrency wallet

Keylogging targets

Package Name	Application Label
com.whatsapp	WhatsApp Messenger
com.viber.voip	Viber Messenger - Messages, Group Chats & Calls
com.zhiliaoapp.musically	TikTok - Make Your Day
com.facebook.katana	Facebook
com.facebook.orca	Messenger – Text and Video Chat for Free
com.facebook.lite	Facebook Lite
