Anubis Targets 250 Android Apps with Ransomware | Cofense

Published: 2020-02-05 · Archived: 2026-04-05 20:47:56 UTC

Retarus Email Security

By Marcel Feller

The Cofense Phishing Defense Center uncovered a phishing campaign that specifically targets users of Android devices that could result in compromise if unsigned Android applications are permitted on the device.

The campaign seeks to deliver Anubis, a particularly nasty piece of malware that was originally used for cyber espionage and retooled as a banking trojan. Anubis can completely hijack an Android mobile device, steal data, record phone calls, and even hold the device to ransom by encrypting the victim's personal files. With mobile devices increasingly used in the corporate environment, thanks to the popularity of BYOD policies, this malware has the potential to cause serious harm, mostly to consumers, and businesses that allow the installation of unsigned applications.

Here's how it works:

At first glance, the email shown in Figure 1 looks like any other phishing email that asks the user to download an invoice. However, this particular email downloads an Android Package Kit (APK), which is the common format used by Android to distribute and install applications. Let's take a closer look at the suspicious file.

Figure 1 – Phishing Email

When the email link is opened from an Android device, an APK file (Fattura002873.apk), is downloaded. Upon opening the file, the user is asked to enable "Google Play Protect" as shown in Figure 2. However, this is not a genuine "Google Play Protect" screen; instead it gives the app all the permissions it needs while simultaneously disabling the actual Google Play Protect.

Figure 2 – Granting Permissions

The following permissions are granted to the app:

Figure 3 – Permissions Granted to App

A closer look at the code reveals the application gathers a list of installed applications to compare the results against a list of targeted applications (Figure 4). The malware mainly targets banking and financial applications, but also looks for popular shopping apps such as eBay or Amazon. A full list of targeted applications is included in the IOC section at the end of this post. Once an application has been identified, Anubis overlays the original application with a fake login page to capture the user's credentials.

Figure 4 – Checking for installed apps

Based on a thorough analysis of the code, the most interesting technical capabilities include:

- Capturing screenshots
- Enabling or changing administration settings
- Opening and visiting any URL
- Disabling Play Protect
- Recording audio
- Making phone calls
- Stealing the contact list
- Controlling the device via VNC
- Sending, receiving and deleting SMS
- Locking the device
- Encrypting files on the device and external drives
- Searching for files
- Retrieving the GPS location
- Capturing remote control commands from Twitter and Telegram
- Pushing overlays
- Reading the device ID

The malware includes a keylogger that works in every app installed on the Android device. However, the keylogger needs to be specifically enabled by a command sent from the C2 server. The keylogger can track three different events (Figure 5):

TYPE_VIEW_CLICKED	Represents the event of clicking on a View-like Button, CompoundButton, etc.
TYPE_VIEW_FOCUSED	Represents the event of setting input focus of a View.
TYPE_VIEW_TEXT_CHANGED	Represents the event of changing the text of an EditText.

Figure 5 – Keylogger component

Figure 6 shows one of the most noteworthy functions of Anubis: its ransomware module. The malware searches both internal and external storage and encrypts them using RC4. It adds the file extension .AnubisCrypt to each encrypted file and sends it to the C2.

Figure 6 – Ransomware component

Anubis has been known to utilize Twitter or Telegram to retrieve the C2 address and this sample is no exception (Figure 7).

Figure 7 – C2

As seen in Figure 8, this version of Anubis is built to run on several iterations of the Android operating system, dating back to version 4.0.3, which was released in 2012.

Figure 8 – Android requirements

Android malware has been around for many years and will be with us for the foreseeable future. Users who have configured their Android mobile device to receive work-related emails and allow installation of unsigned applications face the most risk of compromise. APK files will not natively open in an environment other than an Android device. With the increased use of Android phones in business environments, it is important to defend against these threats by ensuring devices are kept current with the latest updates. Limiting app installations on corporate devices, as well as ensuring that applications are created by trusted developers on official marketplaces, can help in reducing the risk of infection as well.

Indicators of Compromise4.0.3 or newerFile Name: Fattura002873.apk

MD5: c027ec0f9855529877bc0d57453c5e86

SHA256: c38c675a4342052a18e969e839cce797fef842b9d53032882966a3731ced0a70

File Size: 575,236 bytes (561K)hXXp://g28zjbmuc[.]pathareshubhmangalkaryalay[.]com
hXXp://73mw001b0[.]pragatienterprises[.]in[.]net/
hXXp://hrlny7si9[.]pathareshubhmangalkaryalay[.]com/
hXXp://w0puz47[.]arozasehijos[.]cl/
hXXp://hovermop[.]com/Fattura002873[.]apk
hXXps://twitter[.]com/qweqweqwe
hXXp://ktosdelaetskrintotpidor[.]com
hXXp://sositehuypidarasi[.]com
hXXp://cdnjs[.]su/fafa[.]php?f=
hXXp://cdnjs[.]su/o1o/a1[.]php
hXXp://cdnjs[.]su/o1o/a10[.]php
hXXp://cdnjs[.]su/o1o/a11[.]php
hXXp://cdnjs[.]su/o1o/a12[.]php
hXXp://cdnjs[.]su/o1o/a13[.]php
hXXp://cdnjs[.]su/o1o/a14[.]php
hXXp://cdnjs[.]su/o1o/a15[.]php
hXXp://cdnjs[.]su/o1o/a16[.]php
hXXp://cdnjs[.]su/o1o/a2[.]php
hXXp://cdnjs[.]su/o1o/a3[.]php
hXXp://cdnjs[.]su/o1o/a4[.]php
hXXp://cdnjs[.]su/o1o/a5[.]php
hXXp://cdnjs[.]su/o1o/a6[.]php
hXXp://cdnjs[.]su/o1o/a7[.]php
hXXp://cdnjs[.]su/o1o/a8[.]php
hXXp://cdnjs[.]su/o1o/a9[.]phpat.spardat.bcrmobile
at.spardat.netbanking
com.bankaustria.android.olb
com.bmo.mobile

com.cibc.android.mobi
com.rbc.mobile.android
com.scotiabank.mobile
com.td
cz.airbank.android
eu.inmite.prj.kb.mobilbank
com.bankinter.launcher
com.kutxabank.android
com.rsi
com.tecnocom.cajalaboral
es.bancopopular.nbmpopular
es.evobanco.bancamovil
es.lacaixa.mobile.android.newwapicon
com.dbs.hk.dbsmbanking
com.FubonMobileClient
com.hangseng.rbmobile
com.MobileTreeApp
com.mtel.androidbea
com.scb.breezebanking.hk
hk.com.hsbc.hsbchkmobilebanking
com.aff.otpdirekt
com.ideomobile.hapoalim
com.infrasofttech.indianBank
com.mobikwik_new
com.oxigen.oxigenwallet
jp.co.aeonbank.android.passbook
jp.co.netbk
jp.co.rakuten_bank.rakutenbank
jp.co.sevenbank.AppPassbook
jp.co.smbc.direct
jp.mufg.bk.applisp.app
com.barclays.ke.mobile.android.ui
nz.co.anz.android.mobilebanking
nz.co.asb.asbmobile
nz.co.bnz.droidbanking
nz.co.kiwibank.mobile
com.getingroup.mobilebanking
eu.eleader.mobilebanking.pekao.firm
eu.eleader.mobilebanking.raiffeisen
pl.bzwbk.bzwbk24
pl.ipko.mobile
pl.mbank

alior.bankingapp.android
com.comarch.mobile.banking.bgzbnpparibas.biznes
com.comarch.security.mobilebanking
com.empik.empikapp
com.finanteq.finance.ca
com.orangefinansek
eu.eleader.mobilebanking.invest
pl.aliorbank.aib
pl.allegro
pl.bosbank.mobile
pl.bph
pl.bps.bankowoscmobilna
pl.bzwbk.ibiznes24
pl.bzwbk.mobile.tab.bzwbk24
pl.ceneo
pl.com.rossmann.centauros
pl.fmbank.smart
pl.ideabank.mobilebanking
pl.ing.mojeing
pl.millennium.corpApp
pl.orange.mojeorange
pl.pkobp.iko
pl.pkobp.ipkobiznes
com.kuveytturk.mobil
com.magiclick.odeabank
com.mobillium.papara
com.pozitron.albarakaturk
com.teb
com.tmob.denizbank
com.vakifbank.mobilel
tr.com.sekerbilisim.mbank
wit.android.bcpBankingApp.millenniumPL
com.advantage.RaiffeisenBank
hr.asseco.android.jimba.mUCI.ro
may.maybank.android
ro.btrl.mobile
com.amazon.mShop.android.shopping
ru.sberbankmobile
ru.alfabank.mobile.android
ru.mw
com.idamob.tinkoff.android
com.ebay.mobile

ru.vtb24.mobilebanking.android
com.akbank.android.apps.akbank_direkt
com.ykb.android
com.softtech.iscek
com.finansbank.mobile.cepsube
com.garanti.cepsubesi
com.tmobtech.halkbank
com.ziraat.ziraatmobil
de.comdirect.android
de.commerzbanking.mobil
de.consorsbank
com.db.mm.deutschebank
de.dkb.portalapp
com.ing.diba.mbbr2
de.postbank.finanzassistent
mobile.santander.de
de.fiducia.smartphone.android.banking.vr
fr.creditagricole.androidapp
fr.axa.monaxa
fr.banquepopulaire.cyberplus
net.bnpparibas.mescomptes
com.boursorama.android.clients
com.caisseepargne.android.mobilebanking
fr.lcl.android.customerarea
com.paypal.android.p2pmobile
com.konylabs.capitalone
com.chase.sig.android
com.infonow.bofa
com.wf.wellsfargomobile
uk.co.bankofscotland.businessbank
com.rbs.mobile.android.natwestoffshore
uk.co.santander.santanderUK
com.usbank.mobilebanking
com.usaa.mobile.android.usaa
com.suntrust.mobilebanking
com.moneybookers.skrillpayments.neteller
com.clairmail.fth
com.ifs.banking.fiid4202
com.rbs.mobile.android.ubr
com.htsu.hsbcpersonalbanking
com.grppl.android.shell.halifax
com.grppl.android.shell.CMBlloydsTSB73

com.barclays.android.barclaysmobilebanking
sk.sporoapps.accounts
com.cleverlance.csas.servis24
com.unionbank.ecommerce.mobile.android
com.ing.mobile
com.snapwork.hdfc
com.sbi.SBIFreedomPlus
hdfcbank.hdfcquickbank
com.csam.icici.bank.imobile
in.co.bankofbaroda.mpassbook
com.axis.mobile
cz.csob.smartbanking
cz.sberbankcz
org.westpac.bank,nz.co.westpac
au.com.suncorp.SuncorpBank
org.stgeorge.bank
org.banksa.bank
au.com.newcastlepermanent
au.com.nab.mobile
au.com.mebank.banking
au.com.ingdirect.android
com.imb.banking2
com.commbank.netbank
com.citibank.mobile.au
com.fusion.ATMLocator
org.bom.bank
au.com.cua.mb
com.anz.android.gomoney
com.bendigobank.mobile
com.bbva.bbvacontigo
com.bbva.netcash
au.com.bankwest.mobile
com.cm_prod.bad
mobi.societegenerale.mobile.lappli
at.bawag.mbanking
com.pozitron.iscep
com.bankofqueensland.boq
com.starfinanz.smob.android.sfinanzstatus
fr.laposte.lapostemobile
com.starfinanz.smob.android.sbanking
at.easybank.mbanking
com.palatine.android.mobilebanking.prod

at.volksbank.volksbankmobile
com.isis_papyrus.raiffeisen_pay_eyewdg
es.cm.android
com.jiffyondemand.user
com.latuabancaperandroid
com.latuabanca_tabperandroid
com.lynxspa.bancopopolare
com.unicredit
it.bnl.apps.banking
it.bnl.apps.enterprise.bnlpay
it.bpc.proconl.mbplus
it.copergmps.rt.pf.android.sp.bmps
it.gruppocariparma.nowbanking
it.ingdirect.app
it.nogood.container
it.popso.SCRIGNOapp
posteitaliane.posteapp.apppostepay
com.abnamro.nl.mobile.payments
com.triodos.bankingnl
nl.asnbank.asnbankieren
nl.snsbank.mobielbetalen
com.btcturk
com.ingbanktr.ingmobil
finansbank.enpara
tr.com.hsbc.hsbcturkey
com.att.myWireless
com.vzw.hss.myverizon
aib.ibank.android
com.bbnt
com.csg.cs.dnmbs
com.discoverfinancial.mobile
com.eastwest.mobile
com.fi6256.godough
com.fi6543.godough
com.fi6665.godough
com.fi9228.godough
com.fi9908.godough
com.ifs.banking.fiid1369
com.ifs.mobilebanking.fiid3919
com.jackhenry.rockvillebankct
com.jackhenry.washingtontrustbankwa
com.jpm.sig.android

com.sterling.onepay
com.svb.mobilebanking
org.usemployees.mobile
pinacleMobileiPhoneApp.android
com.fuib.android.spot.online
com.ukrsibbank.client.android
ru.alfabank.mobile.ua.android
ua.aval.dbo.client.android
ua.com.cs.ifobs.mobile.android.otp
ua.com.cs.ifobs.mobile.android.pivd
ua.oschadbank.online
ua.privatbank.ap24
com.Plus500
eu.unicreditgroup.hvbapptan
com.targo_prod.bad
com.db.pwcc.dbmobile
com.db.mm.norisbank
com.bitmarket.trader
com.plunien.poloniex
com.mycelium.wallet
com.bitfinex.bfxapp
com.binance.dev
com.binance.odapplications
com.blockfolio.blockfolio
com.crypter.cryptocyrrency
io.getdelta.android
com.edsoftapps.mycoinsvalue
com.coin.profit
com.mal.saul.coinmarketcap
com.tnx.apps.coinportfolio
com.coinbase.android
de.schildbach.wallet
piuk.blockchain.android
info.blockchain.merchant
com.jackpf.blockchainsearch
com.unocoin.unocoinwallet
com.unocoin.unocoinmerchantPoS
com.thunkable.android.santoshmehta364.UNOCOIN_LIVE
wos.com.zebpay
com.localbitcoinsmbapp
com.thunkable.android.manirana54.LocalBitCoins
com.localbitcoins.exchange

com.coins.bit.local
com.coins.ful.bit
com.jamalabbasii1998.localbitcoin
zebpay.Application
com.bitcoin.ss.zebpayindia
com.kryptokit.jaxx**HOW COFENSE CAN HELP**

Every day, the Cofense Phishing Defense Center analyzes phishing emails with malware payloads found in protected email environments. 100% of the threats found by the Cofense PDC were identified by the end user. 0% were stopped by technology.

Condition users to be resilient to evolving phishing attacks with Cofense PhishMe and remove the blind spot with Cofense Reporter. Cofense PhishMe offers a simulation template, "Electricity Bill Invoice – Anubis – Italian," to educate users on the phishing tactic described in this blog.

Quickly turn user reported emails into actionable intelligence with Cofense Triage. Reduce exposure time by rapidly quarantining threats with Cofense Vision.

Easily consume phishing-specific threat intelligence to proactively defend your organization against evolving threats with Cofense Intelligence. Cofense Intelligence customers received further information about this threat in Active Threat Report (ATR) 33675 and the YARA Rule PM_Intel_Anubis_33675.

Thanks to our unique perspective, no one knows more about providing phishing awareness training and REAL phishing threats than Cofense. To understand them better, read the 2019 Phishing Threat & Malware Review.
