feedzai | Report

Coper Malware Analysis

Contents

feedzai

Description of the Coper Family

Coper (also known as Octo) malware applications have a modular design and include a multi-stage infection method and many defensive tactics to evade removal attempts. The Coper malware was initially discovered targeting Colombian users around July 2021.

New versions of the Coper Trojan have been observed targeting Android users in different countries in Europe. They are expected to expand their reach to other regions in the future, targeting a variety of banking apps around the world.

This type of malware was generally known to impersonate apps from the Bancolombia financial institution, but now affects more than 300 institutions worldwide. New versions of the Coper malware have also started to spoof utility applications.

The samples analysed include a library containing the malicious code, which is obfuscated to make it difficult to analyse.

Permissions Requested

Step 1

The trojan calls the GetSystemService api to get information about android services:

- android.os.BatteryManager@7baf2b0
- android.app.ActivityManager@730f5f3
- android.app.AppOpsManager@b29c062
- android.app.NotificationManager@61e193f
- android.app.KeyguardManager@d455640
- android.view.WindowManagerImpl@27a1583

Step 2

Repeatedly checks that it has **all permissions**:

- android.permission.RECEIVE_SMS”
- android.permission.READ_SMS”
- “android.permission.RECEIVE_SMS”
- “android.permission.READ_SMS”
- “android.permission.CALL_PHONE”
- “android.permission.SEND_SMS”
- android.app.NotificationManager@61e193f

Step 3

It also registers the receiver when the battery changes via “android.content.
ContextWrapperregisterReceiver”:

{“action”:”android.intent.action.BATTERY_CHANGED”,”extras”:”{“technology”
:”Li-poly”, “icon-small”:”17303443”, “max_charging_voltage”:”0”, “health”:”2”,
“max_charging_current”:”0”, “status”:”3”, “plugged”:”0”, “present”:”true”,
“seq”:”3”, “charge_counter”:”0”, “level”:”76”, “scale”:”91”, “temperature”:”325”,
“voltage”:”4086”, “invalid_charger”:”0”}”}

Loading the included library

```
static {
    System.loadLibrary("nIqEjTlnW");
}
```

Step 4

Subsequently, it loads the library in which the following functionalities are included:

- Call and phone number monitoring
- Incoming SMS monitoring
- Maintains persistence on reboot

Step 5

The Trojan also checks if it is running in a virtual environment, checks if there is an active SIM card and also checks the user’s country of residence. If one of these checks fails, the droppers will immediately stop working.

Full list of permissions requested

- android.permission.GET_PACKAGE_SIZE
- android.permission.INSTALL_SHORTCUT
- android.permission.INTERNET
- android.permission.MODIFY_AUDIO_SETTINGS
- android.permission.READ_EXTERNAL_STORAGE
- android.permission.READ_PHONE_STATE
- android.permission.READ_SMS
- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.RECEIVE_SMS
- android.permission.REORDER_TASKS
- android.permission.REQUEST_COMPANION_RUN_IN_BACKGROUND
- android.permission.REQUEST_COMPANION_USE_DATA_IN_BACKGROUND
- android.permission.REQUEST_DELETE_PACKAGES
- android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
- android.permission.SEND_RESPOND_VIA_MESSAGE
- android.permission.SEND_SMS
- android.permission.USES_POLICY_FORCE_LOCK
- android.permission.USE_FINGERPRINT
- android.permission.VIBRATE
- android.permission.WAKE_LOCK
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.WRITE_SETTINGS

Communication with C2

First, the malware contacts “ip-api.com/json” via HTTP to obtain the IP of the device where it is running and thus bypass other checks and hooks. After this request, it sends the information about the system where it is running to C2:

```
7b, 22, 78, 63, 22, 3a, 22, 67, 53, 57, 49, 22, 2c, 22, 6c, 42, 22, 3a, 22, 41, 66, 64, 65, 6c, 69, 6e, 67, 22, 2c, 22, 62, 49, 22, 3a, 22,
65, 63, 66, 35, 38, 63, 36, 61, 32, 64, 37, 66, 63, 36, 32, 39, 64, 30, 61, 64, 66, 36, 33, 38, 31, 64, 38, 66, 38, 34, 33, 38, 22, 2c, 22,
69, 41, 22, 3a, 22, 31, 22, 2c, 22, 64, 41, 22, 3a, 22, 31, 22, 2c, 22, 6c, 4b, 22, 3a, 22, 30, 22, 2c, 22, 69, 41, 63, 22, 3a, 22, 31, 22,
2c, 22, 69, 50, 61, 22, 3a, 22, 30, 22, 2c, 22, 69, 42, 43, 22, 3a, 30, 2c, 22, 69, 43, 50, 22, 3a, 22, 30, 22, 2c, 22, 69, 53, 45, 22, 3a,
22, 31, 22, 2c, 22, 69, 53, 70, 22, 3a, 30, 2c, 22, 69, 46, 70, 22, 3a, 22, 22, 2c, 22, 63, 54, 73, 6b, 22, 3a, 22, 64, 69, 73, 61, 62, 6c,
65, 5f, 67, 70, 22, 2c, 22, 75, 70, 22, 3a, 30, 2c, 22, 6b, 4c, 22, 3a, 22, 30, 22, 2c, 22, 76, 6e, 63, 22, 3a, 22, 22, 2c, 22, 66, 67, 4d,
22, 3a, 22, 30, 22, 2c, 22, 69, 41, 67, 22, 3a, 66, 61, 6c, 73, 65, 2c, 22, 72, 49, 50, 22, 3a, 22, 33, 34, 2e, 38, 35, 2e, 31, 35, 31, 2e,
31, 36, 31, 3b, 20, 55, 6e, 69, 74, 65, 64, 20, 53, 74, 61, 74, 65, 73, 3b, 20, 57, 61, 73, 68, 69, 6e, 67, 74, 6f, 6e, 2c, 20, 44, 2e, 43,
2e, 3b, 20, 57, 61, 73, 68, 69, 6e, 67, 74, 6f, 6e, 3b, 20, 47, 6f, 6f, 67, 6c, 65, 20, 4c, 4c, 43, 22, 7d
```

```
{"xc":"bR","tA":"3ce00749dd913534","tB":"","tC":"us","tD":"en","tE":"8.1.0","tF":"QEMU Standard PC (i440FX + PIIX,
1996)","tG":"ATT","lA":"com.android.cts.priv.ctsshim|com.google.android.youtube|com.google.android.ext.services|
com.example.android.rssreader|com.android.providers.telephony|org.android_x86.analytics|com.google.android.googlequicksearchbox|
com.android.providers.calendar|com.android.providers.media|com.google.android.onetimeinitializer|com.google.android.ext.shared|
com.android.wallpapercropper|org.zeroxlab.util.tscal|com.android.documentsui|com.android.externalstorage|com.android.htmlviewer|
com.android.companiondevicemanager|com.android.mms.service|com.android.providers.downloads|com.android.defcontainer|
com.android.providers.downloads.ui|com.android.vending|com.android.pacprocessor|com.android.certinstaller|com.android.carrierconfig|
android|com.android.contacts|com.android.camera2|com.android.egg|com.android.mtp|com.android.launcher3|com.android.backupconfirm|
com.android.statementservice|com.google.android.gm|com.thenblue2|com.android.calendar|com.android.systemui.theme.dark|
com.google.android.setupwizard|com.android.providers.settings|com.android.sharedstoragebackup|com.android.printspooler|
com.android.dreams.basic|com.android.inputdevices|com.android.bips|com.android.cellbroadcastreceiver|com.google.android.webview|
com.google.android.syncadapters.contacts|com.example.android.notepad|com.android.keychain|com.android.chrome|com.android.dialer|
com.android.gallery3d|com.google.android.packageinstaller|com.google.android.gms|com.google.android.gsf|com.android.calllogbackup|
com.google.android.partnersetup|com.android.basicsmsreceiver|com.android.carrierdefaultapp|com.svox.pico|com.android.proxyhandler|
com.android.inputmethod.latin|org.lineageos.eleven|com.google.android.feedback|com.google.android.printservice.recommendation|
com.google.android.syncadapters.calendar|com.android.managedprovisioning|com.android.providers.partnerbookmarks|
com.google.android.gsf.login|com.android.wallpaper.livepicker|com.google.android.backuptransport|com.android.storagemanager|
com.android.bookmarkprovider|com.android.settings|com.farmerbb.taskbar.androidx86|com.android.calculator2|com.google.android.apps.books|
com.android.cts.ctsshim|com.android.vpndialogs|eu.chainfire.supersu|com.android.phone|com.android.shell|com.android.wallpaperbackup|
com.android.providers.blockednumber|com.android.providers.userdictionary|com.android.emergency|com.android.location.fused|
com.android.deskclock|com.android.systemui|com.android.bluetoothmidiservice|com.termoneplus|com.android.bluetooth|com.android.development|
com.android.wallpaperpicker|com.android.providers.contacts|
com.android.captiveportallogin|","lB":"Afdeling","bI":"ecf58c6a2d7fc629d0adf6381d8f8438","iA":"1","dA":"1","lK":"0","iAc":"1","iPa":"0","i
BC":0,"iCP":"0","iSE":"1","iSp":0,"iFp":"","cTsk":"disable_gp","up":0,"kL":"0","vnc":"","fgM":"0","iAg":false,"rIP":"[redacted] United
States; Washington, D.C.; Washington; Google LLC"}
```

You get as a **first response**:

```
6v23FBePoOHfMwn/JMNXC6Xskf9h50vk6w8bTd9BUem2/RGScqcRaSFT
VBAWLiCh3SEXtIqLxzmJ6ciQjiQiiGpdllSuWo+2EdgsjM7Ihpfd3WVanFDHALY
8VEk/m8eT
```

After deciphering it, it corresponds to:

```
{“response”:”er1”,”tasks”:[],”panel_smarts_ver”:”46”,”keylogger_enabled”:
null,”net_delay”:”60”}
```

Corresponds to the initial configuration of the version (46), the delay between requests and the activation of the keylogger.

The **C2** registers the victim and once the **receiver_Registered** and the **acsb_system_init** are completed it returns the list of applications to attack.

To communicate with C2 it uses a **double encryption system** where it first calls the constructor with the following key:

```
java.crypto.spec.SecretKeySpec $init
["35, 34, 35, 36, 39, 64, 32, 61, 61, 61, 65, 37, 31, 37, 36, 33, 33, 35, 61, 36, 37, 62,
66, 37, 32, 65, 38, 36, 37, 33, 36, 66","AES"] = 54569d2aaae7176335a67bf72e86
736f KEY
```

Y posteriormente llama a **android.util.Base64.encode()** para enviarlo al servidor remoto.

The **configuration** and its **updates** are stored in **/data/data/<PACKAGE>/main.xml** and before replacing it, save a temporary backup in **"/data/user/0/com.thenblue2/shared_prefs/main.xml.bak**".

Requests are made via org.apache.http:

```
["{"method":"POST","url":"https://sdhfsdbfbjhsdhff.com/ZTYxYWI2NWNmY
TA3/","headers":{}}"]
```

When all checks have been completed and C2 validates the communications, it returns the list of banks to be attacked together with the status "OK REG_SUCCESS".

C2:

HTTP Requests
https://ssgsjhfsffdsjhd.info/ZTYxYWI2MWNmYTA3/
https://ssdhfsdbfbjhsdhff.com/ZTYxYWI2MWNmYTA3/
https://dfdfdfdgdffjdhbf.org/ZTYxYWI2MWNmYTA3/
https://www.ip-api.com/json

DNS Requests
www.ip-api.com

Configuration

Coper saves the following information from the system, to be sent in the following keys:

- **installed_pkgs:** sends an '|' separated list of all installed APKs on the system
- **real_ip:** sends the IP and ISP information
- **acsb_system_init:** indicates that the routine to disable all security mechanisms has been started.
- **smart_injects:** apply a generic pattern on gmail
- **keylogger_enabled:** indicates that the keylogger has been enabled.
- **is_registered**
- **smarts_attempts:** how many times it has tried to steal credentials using generic inj
- **keylogger_delay:** time from when the keylogger is started until it starts logging in
- **block_push_delay:** time it takes to apply overlays on target app
- **block_push_apps:** apps to monitor
- **inj_acsb:** automatism to configure the settings
- **uptime:** time in execution
- **minimize_apps:** applications minimised when detected
- **minimze_delay:** delay to minimize antivirus applications
- **component_pkg_name:** installed package name
- **receiver_Registered:** records whether persistence has been successfully enabled
- **net_delay:** time to make the next request
- **injects_delay:** time to apply injects in target apps
- **last_server:** stores the data of the last rotated server
- **domains:** stores the list of C2 to rotate separated by '|'

Affected Entities

The list of financial institutions affected by Coper has grown over time. All known modifications of the Coper banker Trojan have so far targeted Colombian users. However, we have detected how they have overwhelmingly expanded the list of **entities targeted, targeting European entities and cryptocurrency exchanges**.

After analysing the sample, we have obtained the list of more than **300 affected entities**.

Affected Apps/Entities

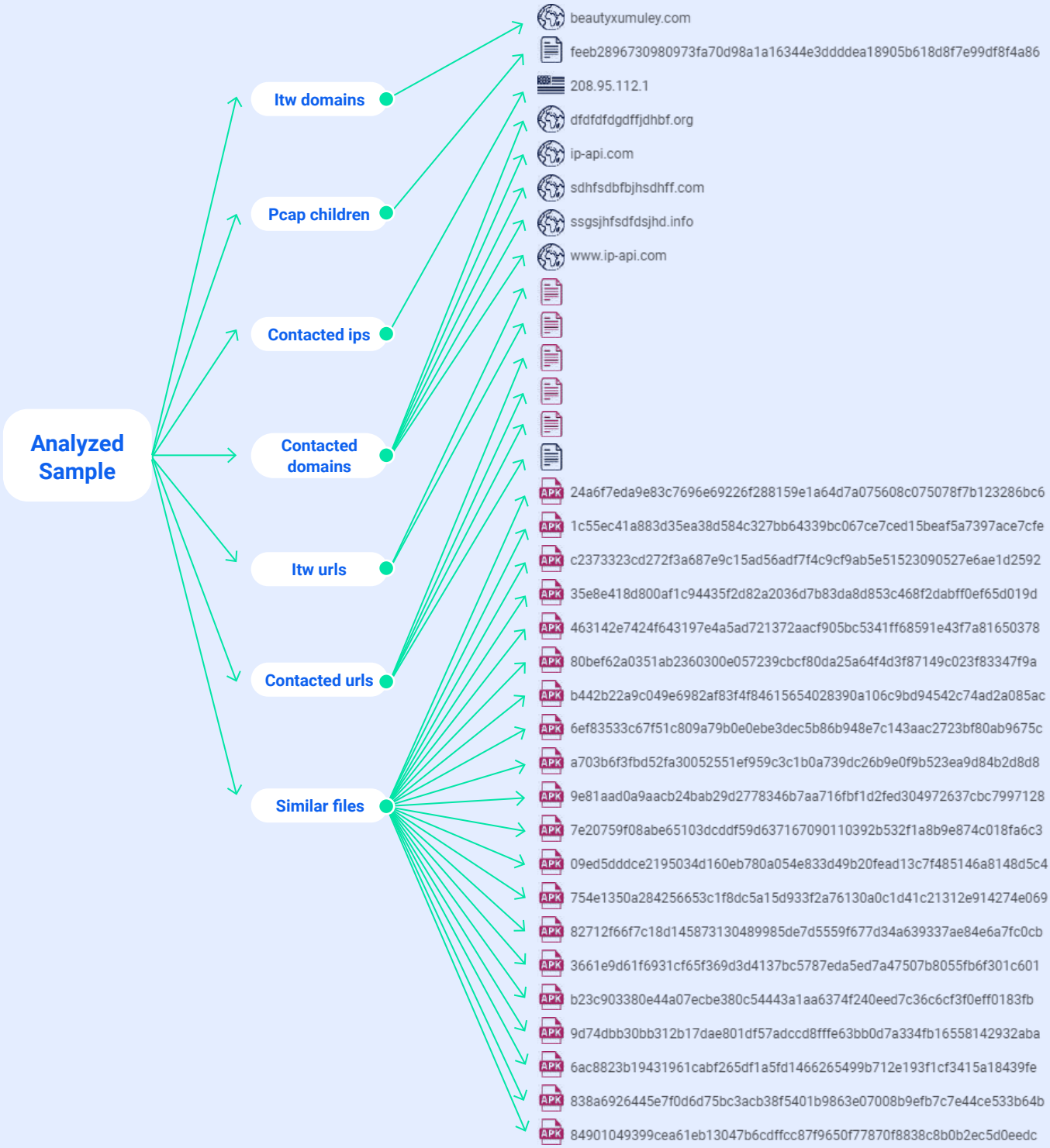
at.spardat.bcrmobile,at.spardat.netbanking,com.bankaustria.android.olb,com.bmo.mobile,com.cibc.android.mobi,com.rbc.mobile.android,com.scotiabank.mobile,com.td,cz.airbank.android,eu.inmite.prj.kb.mobilbank,com.bankinter.launcher,com.kutxabank.android,com.rsi,com.tecnocom.cajalaboral,es.bancopopular.nbmpopular,es.evobanco.bancamovil,es.lacaixa.mobile.android.newwapicon,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.pekao,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.empik.empikfoto,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,ccom.tmob.denizbank,com.tmob.tabletdeniz,com.vakifbank.mobilel,tr.com.sekerbilisim.mbank,wit.android.bcpBankingApp.millenniumPL,com.idamobile.android.hcb,logo.com.mbanking,com.openbank,com.google.android.apps.walletnfcrel,com.samsung.android.spay,com.cardsapp.android,cz.bsc.rc,cb.ibank,com.bifit.mobile.ubrr,com.bssys.mbcphone.ubrir,net.bl,com.bifit.mobile.bin,com.webmoney.my,com.polehin.android,com.bitcoin.mwallet,io.totalcoin.wallet,com.quppy,com.sharpdev.fxcoin,com.advantage.RaiffeisenBank,hr.asseco.android.jimba.mUCI.ro,may.maybank.android,ro.btrl.mobile,com.amazon.mShop.android.shopping,com.amazon.windowshop,com.ebay.mobile,com.idamob.tinkoff.android,com.akbank.android.apps.akbank_direkt,com.akbank.android.apps.akbank_direkt_tablet,com.akbank.softotp,com.akbank.android.apps.akbank_direkt_tablet_20,com.fragment.akbank,com.ykb.android,com.ykb.android.mobilonay,com.ykb.avm,com.ykb.androidtablet,com.veripark.ykbaz,com.softtech.iscek,com.yurtdisi.iscep,com.softtech.isbankasi,com.monitise.isbankmoscow,com.finansbank.mobile.cepsube,finansbank.enpara,com.magiclick.FinansPOS,com.matriksdata.finansyatirim,finansbank.enpara.sirketim,com.vipera.ts.starter.QNB,com.redrockdigimark,com.garanti.cepsubesi,com.garanti.cepbank,com.garantibank.cepsubesiro,biz.mobinex.android.apps.cep_sifrematik,com.garantiyatirim.fx,com.tmobtech.halkbank,com.SifrebazCep,eu.newfrontier.iBanking.mobile.Halk.Retail,tr.com.tradesoft.tradingsystem.gtpmobile.halk,com.DijitalSahne.EnYakinHalkbank,com.ziraat.ziraatmobil,com.ziraat.ziraattablet,com.matriksmobile.android.ziraatTrader,com.matriksdata.ziraatyatirim.pad,de.ingdiba.bankingapp,de.comdirect.android,de.commerzbanking.mobil,de.consorsbank,com.db.mm.deutschebank,de.dkb.portalapp,com.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.c ustomerarea,com.paypal.android.p2pmobile,com.wf.wellsfargomobile,com.wf.wellsfargomobile.tablet,com.wellsFargo.ceomobile,com.usbank.mobilebanking,com.usaa.mobile.android.usaa,com.suntrust.mobilebanking,com.moneybookers.skrillpayments.neteller,com.moneybookers.skrillpayments,com.clairmail.fth,com.konylabs.capitalone,com.yinzcam.facilities.verizon,com.chase.sig.android,com.infonow.bofa,com.bankofamerica.cashpromobile,uk.co.bankofscotland.businessbank,com.grppl.android.shell.BOS,com.rbs.mobile.android.natwestoffshore,com.rbs.mobile.android.natwest,com.rbs.mobile.android.natwestbandc,com.rbs.mobile.investisir,com.phyder.engage,com.rbs.mobile.android.rbs,com.rbs.mobile.android.rbsbandc,uk.co.santander.santanderUK,uk.co.

santander.businessUK.bb,com.sovereign.santander,com.ifs.banking.fiid4202,com.fi6122.godough,com.rbs.mobile.android.ubr,com.htsu.hsbcpersonalbanking,com.grppl.android.shell.halifax,com.grppl.android.shell.CMBlloydsTSB73,com.barclays.android.barclaysmobilebanking,com.unionbank.ecommerce.mobile.android,com.unionbank.ecommerce.mobile.commercial.legacy,com.snapwork.IDBI,com.idbibank.abhay_card,src.com.idbi,com.idbi.mpassbook,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,sk.sporoapps.accounts,sk.sporoapps.skener,com.cleverlance.csas.servis24,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,MyING.be,com.imb.banking2,com.fusion.ATMLocator,au.com.cua.mb,com.commbank.netbank,com.citibank.mobile.au,com.citibank.mobile.uk,com.citi.citimobile,org.bom.bank,com.bendigobank.mobile,me.doubledutch.hvdnz.cbnationalconference2016,au.com.bankwest.mobile,com.bankofqueensland.boq,com.anz.android.gomoney,com.anz.android,com.anz.SingaporeDigitalBanking,com.anzspot.mobile,com.crowdcompass.appSQ0QACAcYJ,com.arubanetworks.atmanz,com.quickmobile.anzirevents15,at.volksbank.volksbankmobile,it.volksbank.android,it.secservizi.mobile.atime.bpaa,de.fiducia.smartphone.android.securego.vr,com.isis_papyrus.raiffeisen_pay_eyewdg,at.easybank.mbanking,at.easybank.tablet,at.easybank.securityapp,at.bawag.mbanking,com.bawagpsk.securityapp,at.psa.app.bawag,com.pozitron.iscep,com.vakifbank.mobile,com.pozitron.vakifbank,com.starfinanz.smob.android.sfinanzstatus,com.starfinanz.mobile.android.pushtan,com.entersekt.authapp.sparkasse,com.starfinanz.smob.android.sfinanzstatus.tablet,com.starfinanz.smob.android.sbanking,com.palatine.android.mobilebanking.prod,fr.laposte.lapostemobile,com.cm_prod.bad,com.cm_prod.epasal,com.cm_prod_tablet.bad,com.cm_prod.nosactus,mobi.societegenerale.mobile.lappli,com.bbva.netcash,com.bbva.bbvacontigo,com.bbva.bbvawallet,es.bancosantander.apps,com.santander.app,es.cm.android,es.cm.android.tablet,com.bankia.wallet,com.bestbuy.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,com.tmob.denizbank,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,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,com.portfolio.coinbase_tracker,com.bitpay.wallet,com.bitcoin.wallet.btc,com.blocktrail.mywallet,org.electrum.electrum,com.paxful.wallet,com.bitcoin.pocketbook.btc,net.bitstamp.app,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.thunkable.android.manirana54.LocalBitCoins_unblock,com.localbitcoins.exchange,com.coins.bit.local,com.coins.ful.bit,com.jamalabbasii1998.localbitcoin,zebpay.Application,xmr.org.freewallet.app,com.bitcoin.ss.zebpayindia,com.kryptokit.jaxx,com.cajasur.android,app.wizink.es,com.grupocajamar.wefferent,caixagalicia.activamovil,com.abanca.bancaempresas,net.inverline.bancosabadell.officelocator.android,es.caixageral.caixageralapp,com.bankinter.bkwallet,com.db.pbc.mibanco,com.indra.itecban.mobile.novobanco,es.openbank.mobile,es.pibank.customers,es.bancosantander.empresas,com.indra.itecban.triodosbank.mobile.banking,es.univia.unicajamovil,com.westernunion.moneytransferr3app.es,www.ingdirect.nativeframe

Related Information



Conclusion

According to Feedzai's sources, banking Trojans no longer perform attacks only based on 'overlays' or using Mobility as a service (MaaS), as previously detected in numerous banking Trojan malware variants. Some samples analysed also use VNC to launch screen recording services by recognising the foreground configuration in the application list.

Finally, Coper is also able to hide notifications received by banks ipso-facto, as well as having the ability to close applications. It uses this so that permissions cannot be changed.

Financial institutions must prepare for the challenges posed by this virus by understanding the security landscape. This can be achieved by implementing a real-time threat-based mobile security strategy.

> **Financial institutions must prepare for the challenges posed by this virus by understanding the security landscape.**

IOCs

Sample hash

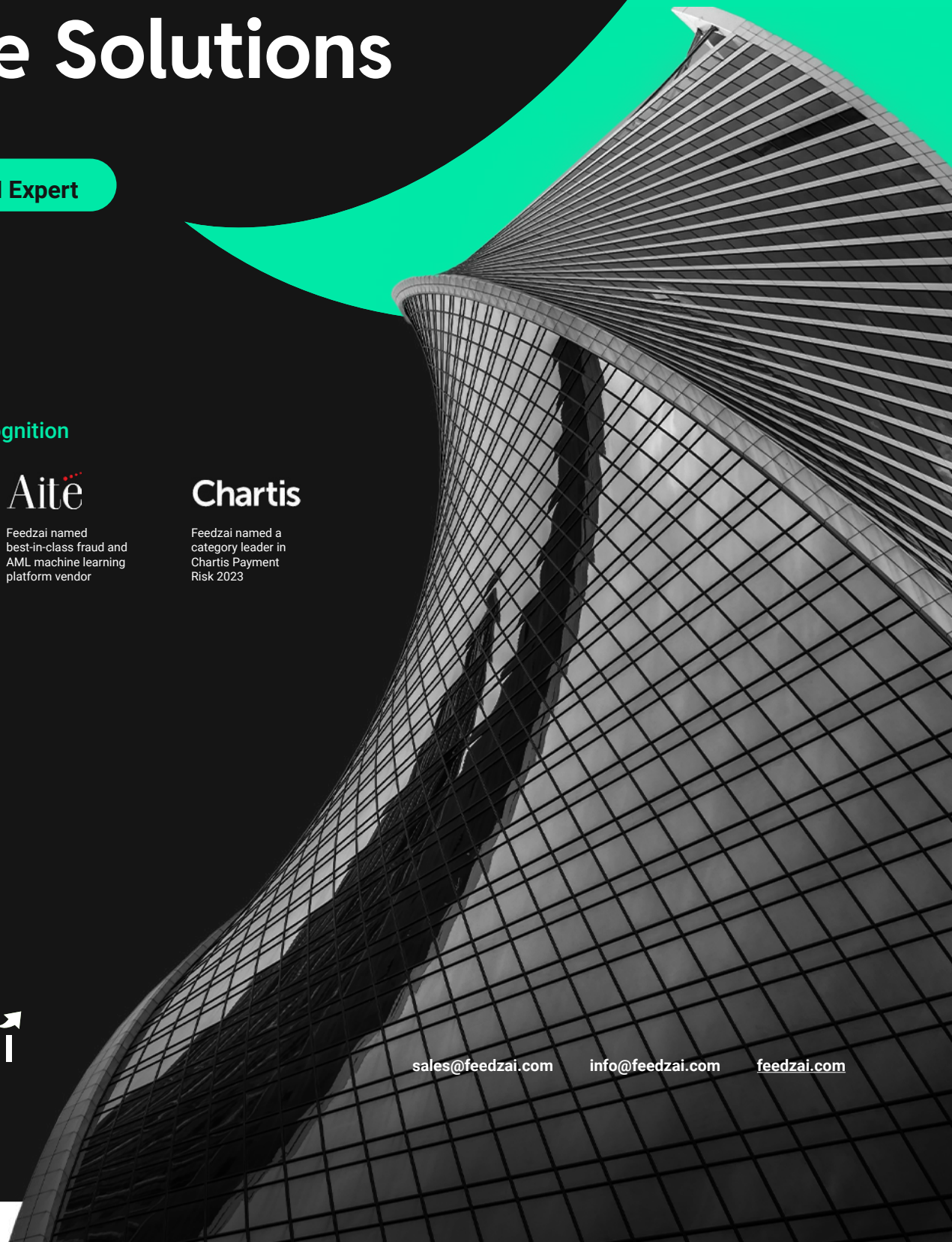
- 7df3e7fcc0dc2e45fedc0615bcf7b9a060e641f4cec7826246786c3864e409c4
- a3a6069f6e901144e9ac1c4353e1b80639aa52bbcbe6a9e47c3badd4425b2764
- 3048df5168dab724ea310f31dbd36cfe8ddebe3376c9c01c93b697e7ace424d4
- 77509e714b925cbd657145157246e995f80ac51d4582733497bb6c25f3bed75a

Domains, IPs and URLs

- https://beautyxumuley.com/
- http://beautyxumuley.com/office/oWa/index.php
- https://ssgsjhfsdfdsjhd.info/ZTYxYWI2NWNmYTA3/
- https://dfdfdfdgdffjdhbf.org/ZTYxYWI2NWNmYTA3/
- https://sdhfsdbfbjhsdhff.com/ZTYxYWI2NWNmYTA3/

Fraud and Financial Crime Solutions

Speak to an AI Expert



Awards and Recognition

Quadrant Knowledge Solutions

Feedzai named a leader in SPARK Matrix AML.

Aité

Feedzai named best-in-class fraud and AML machine learning platform vendor

Chartis

Feedzai named a category leader in Chartis Payment Risk 2023

feedzai

sales@feedzai.com info@feedzai.com feedzai.com