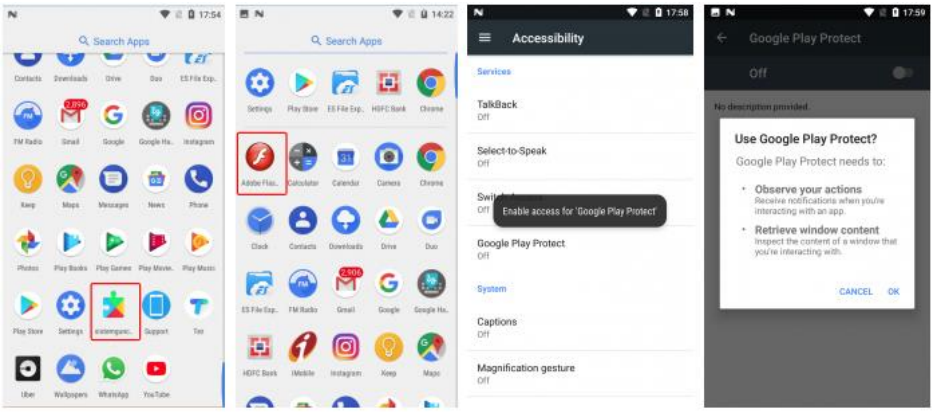
بسمه تعالی

کشف بدافزار خطرناک اندرویدی با قابلیت سرقت اطلاعات بانکی، انتقال تماس و فعالیت‌های باج‌افزاری

محققان Quick Heal یک تروجان جدید اندروید را کشف کردند که شامل قابلیت‌های تروجان بانکداری، انتقال تماس، ضبط صدا، ثبت ضربات کلید و فعالیت‌های باج‌افزاری است. این بدافزار، برنامه‌های بانکی محبوب مانند HFC، ICICI، SBI، Axis Bank و دیگر کیف پول‌های الکترونیکی را هدف قرار داده است.

اپراتور این بدافزار برای موفقیت در حمله، نیاز به تعامل بیشتری با کاربر دارد و تا زمان دسترسی به مجوز "AccessibilityService"، صفحه‌ی تنظیمات دسترسی را به کاربر نمایش می‌دهد. داشتن قابلیت "AccessibilityService" به این بدافزار اجازه می‌دهد تا بدون نیاز به اجازه‌ی کاربر، به همه‌ی مجوزها دسترسی پیدا کند.



شکل 1 صفحه‌ی تنظیمات "AccessibilityService" بازشده توسط بدافزار

به‌گفته‌ی محققان Quick Heal این بدافزار تعدادی از فعالیت‌ها را براساس دستورات دریافت‌شده از سرور C&C انجام می‌دهد که این دستورات در جدول 1 زیر نشان داده شده است.

هنگامی که برنامه‌ی کاربردی هدف راه‌اندازی می‌شود، یک لایه‌ی پوششی حاوی فرم ورود به سیستم ماهیگیری را بر روی پنجره‌ی آن نمایش می‌دهد و اطلاعات محرمانه مانند نام کاربری و رمز عبور را درخواست می‌کند. حملات لایه‌ی پوششی به مهاجم اجازه می‌دهد تا پنجره‌ای را در بالای پنجره‌های دیگر و برنامه‌های در حال اجرا بر روی دستگاه قرار دهد.

این بدافزار، فایل APK اصلی را مورد سوءاستفاده قرار می‌دهد، رشته‌ها را رمزگذاری می‌کند و اطلاعات ناخواسته را اضافه می‌کند تا برای مهندسی معکوس دشوار باشد.

این بدافزار همچنین فعال‌بودن "Play Protect" را بررسی می‌کند و درصورت فعال بودن آن، هشدار جعلی «سیستم به‌درستی کار نمی‌کند، Google Play Protect را غیرفعال کنید» را نمایش می‌دهد و از کاربر می خواهد تا آن را غیرفعال کند.

جدول 1 دستورات استفاده‌شده توسط بدافزار

دستورات	مفهوم
Send_GO_SMS	ارسال پیامک از دستگاه آلوده
nymBePsG0	آپلود تمامی شماره‌ها از دفترچه تلفن به سرور C&C
GetSWSGO	آپلود تمامی پیامک‌ها به سرور C&C
telbookgotext	ارسال پیامک به تمامی شماره‌های موجود در دستگاه آلوده
Getapps	آپلود لیست تمام برنامه‌های نصب‌شده
ALERT	نمایش پیامی که محتویات آن در دستورات مشخص شده است
PUSH	نمایش اعلانی که محتویات آن در دستورات مشخص شده است
startAutoPush	نمایش اعلانی که محتویات آن در کد تروجان تنظیم شده است
ussd	تماس با یک شماره‌ی USSD از دستگاه آلوده
Sockshost	آغاز Server Socket
stopsocks5	توقف Server Socket
Recordsound	آغاز ضبط صدا
Replaceurl	جایگزینی پنل URL
Startapplication	آغاز برنامه‌ای که در دستورات مشخص شده است
killBot	پاک‌کردن آدرس سرور C&C
Getkeylogger	آپلود ورودی‌های ضربات کلید به سرور
Startrat	آغاز Remote Administration Tool
Startforward	آغاز انتقال تماس به شماره‌ی مشخص‌شده در دستورات
Stopforward	توقف انتقال تماس
Openbrowser	بازکردن URL در مرورگر
Openactivity	بازکردن URL در WebView
Cryptokey	رمزگذاری تمامی فایل‌ها
decryptokey	رمزگشایی تمامی فایل‌ها

محققان همچنین متوجه شدند که اگر کاربر تلاش کند تا برنامه‌ی آلوده را پاک کند، بدافزار هشداری را با پیام "System Error 495" نشان می‌دهد.

فعالان این تهدید از حساب توییتر برای ارتباط C&C استفاده می‌کنند. مهاجمان، آدرس سرور رمزگذاری شده‌ی C&C را در توییتر ارسال می‌کنند و بدافزار، آدرس رمزگذاری‌شده را از حساب توییتر دریافت می کند.

اگر بدافزار دستور "cryptokey" را دریافت کند، تمام فایل‌ها را در دستگاه قربانی رمزگذاری می‌کند و آن‌ها را با پسوند ".AnubisCrypt" تغییرنام می‌دهد. هنگامی که رمزگذاری انجام می‌شود، یادداشت دریافت باج نشان داده می‌شود و صفحه‌ی نمایش را با نمایش Window WebView مسدود می‌کند.

Quick Heal این تروجان را "Android.Banker.L" نامیده است و شاخص سازش آن عبارتند از:

نام برنامه: sistemguncelle

نام بسته: com.qvgstiwjsndr.jktqnsyc

MD5: b0ff12e875d1c32bd05dde6bb34e9805

اندازه: 344 کیلوبایت

نام برنامه: Adobe Flash Player

نام بسته: com.fzuhnorsz.xgvmhdztawmg

MD5: bc53a5857b1e29bef175d64fbec0c186

اندازه: 383 کیلوبایت

لیست کامل برنامه‌هایی که هدف این بدافزار قرار گرفته‌اند به شرح زیر است:

- 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