IOC

Samples in Play Store

First Campaign

SHA256	Package Name	Cert SHA1	C2	GP Developer	Uploaded/Removed
89f537cb4495a50b082758b34e54bd1024463176d7d2f4a445cf859f5a33e38f	com.andrtorn.app	f9e35a21aa2ea2e10d22a78b82bfa33e6cb9b46b	138.201.166.31	sandowares@gmail.com	-
d93e03c833bac1a29f49fa5c3060a04298e7811e4fb0994afc05a25c24a3e6dc	com.sysdriver.andr	401b63bd7d211000a0403702a262a76946ccb06d	138.201.166.31	-	-
3a3c5328347fa52383406b6d6ca31337442659ae8fafdff0972703cb49d97ac2	com.sysmonitor.service	83c59d1540e8265e1fe235aa680f2367e33a5acc	138.201.166.31	-	-
138e3199d53dbbaa01db40742153775d54934433e999b9c7fcfa2fea2474ce8d	com.wifimodule.sys	fad67c31eea68431bdffe361fe606c2d1bf53634	138.201.166.31	brandonnash227@gmail.com	Oct 26,17 / Oct 27,17
c1720011300d8851bc30589063425799e4cce9bb972b3b32b6e30c21ce72b9b6	com.seafl.andr	cc50778ef1e1cb945e5da05674277ae59f111626	138.201.166.31	johndohware@gmail.com	Oct16, 17 / -
bb932ca35651624fba2820d657bb10556aba66f15c053142a5645aa8fc31bbd0	com.sarniaps.deew	4e89d0be1c9ec170489b002798aa61b382e6fc44	138.201.166.31	Not in Google Play	-

Payload Downloaded

SHA256	Package Name	Cert SHA1	C2
9a2149648d9f56e999bd5af599d041f00c3130fca282ec47430a3aa575a73dcd	com.vdn.market.plugin.upd	8c84b104a9984e2a93225a7b8d45a4207cc8cfa3	138.201.166.31

Second Campaign

SHA256	Package Name	Cert SHA1	C2	GP Developer	Uploaded/Removed

2058ade23e1d386951d804533701aa3585c0e334abe3e6cd5d2c96395627646c	com.ntoeeemeterp.sever	2e29d6fc3a84b72c42518a518eacd99cab9ed556	88820.pro5.61.32.253		
dd857e8505cedf84b316eb0f5cdcba1386fb8412bc630e671f474aeedfccb387	com.fleeeishei.erabladmounsem	f5624e65d5a895a61c89048559e7f48de036cbdb	88819.pro5.61.32.253		
ef3dfcd3e1351f46ee3cbfb3f71fe9d06a445d8affe2e679f34d8bf4bb618849	com.bucholregaum.hampelpa	54b048c706fa00b6554690b4d8d7abef6a467a3a	5.61.32.253	contact@worldnews.net	-
d2a6cbe9acd4193188f7aa6d922c916999845da8217188952655079 0f5632b47	com.peridesurramant.worldnews	997bd2323ddd88d040860e74ae9f5c72a7adfe94			
3fc104c7fb8f6419aa5b45a3abfcc545ddb8e225f1b6dcaf5824075cbdf5dddd	com.peridesuramant.worldnews	1d4dcd377b10b7667deba521dccc5daf02607fdb			
299cebe015e6bee5e50befd5fd3755ebf4a0cacc0fae354fbd3a603ce54ca99f	com.ntomeeeeeterp.sever	cdf0eba7a95bfc9957bde3e8fefa8ec523b7eb19			
58692776a73e0558da761858a158c279fe2d73e49defeec310709452c8fa211d	com.urbanodevelop.solitaire	8d17cbcb4aedbdc9804ac98d5c1bd957923798d1	5.61.32.253	pronin@classicsolitaire.org	-
b98d3f4950d07f62f22b4c933416a007298f9f38bebb897be0e31e4399eb39c3	com.urbanodevelop.solitaire	8d17cbcb4aedbdc9804ac98d5c1bd957923798d1	5.61.32.253	-	-
cc32d14cea8c9ff13e95d2a83135ae4b7f4b0bd84388c718d324d559180218fd	com.sdssssd.rambooster	c13743d479349575322791434377bfc659552789	5.61.32.253	support@xdccleaner.org	
	com.jduvendc.solitaire			frolikov@solitairecardgame.net	

Payload Downloaded

SHA256	Package Name	Cert SHA1	C2
129e8d59f2e3a6f0ac4c98bfd12f9fb5d38176164ff5cf715e7e082ab33fffb6	com.vdn.market.plugin.upd	8c84b104a9984e2a93225a7b8d45a4207cc8cfa3	-

Hosts

vps.cnucok.com	138.201.166.31, DE
88810.pro 88819.pro 88817.pro 88881.pro 88813.pro 88820.pro 88884.pro	5.61.32.253, DE

Control Panel

h__p://vps·cnucok·com:6008/login	138.201.166.31, DE
h__p://is03·ru:6008/login	138.201.166.31, DE
h__p://static·31·166·201·138·clients·your-server·de:6008/login	138.201.166.31, DE

Targeted Apps

ar.nbad.emobile.android.mobilebank
at.bawag.mbanking
at.spardat.bcrmobile
at.spardat.netbanking

au.com.bankwest.mobile
au.com.cua.mb
au.com.ingdirect.android
au.com.nab.mobile
au.com.newcastlepermanent
au.com.suncorp.SuncorpBank
ch.raiffeisen.android
com.EurobankEFG
com.adcb.bank
com.adib.mbs
com.advantage.RaiffeisenBank
com.akbank.android.apps.akbank_direkt
com.anz.SingaporeDigitalBanking
com.bankaustria.android.olb
com.bankofqueensland.boq
com.bbva.bbvacontigo
com.bbva.netcash
com.bendigobank.mobile
com.caisseepargne.android.mobilebanking
com.cajamar.Cajamar
com.cbd.mobile
com.chase.sig.android
com.citibank.mobile.au
com.cm_prod.bad
com.comarch.mobile
com.comarch.mobile.banking.bnpparibas
com.commbank.netbank
com.csam.icici.bank.imobile
com.csg.cs.dnmb
com.db.mm.deutschebank
com.db.mm.norisbank
com.dib.app
com.finansbank.mobile.cepsube
com.finanteq.finance.ca
com.garanti.cepsubesi
com.getingroup.mobilebanking
com.htsu.hsbcpersonalbanking
com.imb.banking2
com.infonow.bofa
com.ing.diba.mbbr2
com.ing.mobile
com.isis_papyrus.raiffeisen_pay_eyewdg
com.konylabs.capitalone
com.mobileloft.alpha.droid
com.palatine.android.mobilebanking.prod
com.pozitron.iscep
com.rak
com.rsi
com.sbi.SBIFreedomPlus
com.snapwork.hdfc

com.starfinanz.smob.android.sfinanzstatus
com.suntrust.mobilebanking
com.targo_prod.bad
com.tmobtech.halkbank
com.ubs.swidKXJ.android
com.unicredit
com.unionbank.ecommerce.mobile.android
com.usaa.mobile.android.usaa
com.usbank.mobilebanking
com.vakifbank.mobile
com.vipera.ts.starter.FGB
com.vipera.ts.starter.MashreqAE
com.wf.wellsfargomobile
com.ykb.android
com.ziraat.ziraatmobil
cz.airbank.android
cz.csob.smartbanking
cz.sberbankcz
de.comdirect.android
de.commerzbanking.mobil
de.direkt1822.banking
de.dkb.portalapp
de.fiducia.smartphone.android.banking.vr
de.postbank.finanzassistent
de.sdvrz.ihb.mobile.app
enbd.mobilebanking
es.bancosantander.apps
es.cm.android
es.ibercaja.ibercajaapp
es.lacaixa.mobile.android.newwapicon
es.univia.unicajamovil
eu.eleader.mobilebanking.pekao
eu.eleader.mobilebanking.pekao.firm
eu.inmite.prj.kb.mobilbank
eu.unicreditgroup.hvbapptan
fr.banquepopulaire.cyberplus
fr.creditagricole.androidapp
fr.laposte.lapostemobile
fr.lcl.android.customerarea
gr.winbank.mobile
in.co.bankofbaroda.mpassbook
mbanking.NBG
mobi.societegenerale.mobile.lappli
mobile.santander.de
net.bnpparibas.mescomptes
net.inverline.bancosabadell.officelocator.android
nz.co.anz.android.mobilebanking
nz.co.asb.asbmobile
nz.co.bnz.droidbanking
nz.co.kiwibank.mobile

nz.co.westpac
org.banksa.bank
org.bom.bank
org.stgeorge.bank
org.westpac.bank
pl.bzwbk.bzwbk24
pl.bzwbk.ibiznes24
pl.ipko.mobile
pl.mbank
pt.bancobpi.mobile.fiabilizacao
pt.cgd.caixadirecta
pt.novobanco.nbapp
ro.btrl.mobile
src.com.idbi
wit.android.bcpBankingApp.activoBank
wit.android.bcpBankingApp.millennium
wit.android.bcpBankingApp.millenniumPL
www.ingdirect.nativeframe
Com.barclays.ke.mobile.android.ui
Com.scb.breezebanking.hk
com·moneybookers·skrillpayments
com·moneybookers·skrillpayments·neteller