بیش از ۱۰۰ اپلیکیشن مخرب با ۴ میلیون و ۶۰۰ هزار نصب در گوگل پلی

محققان بیش از ۱۰۰ برنامه مخرب را از فروشگاه گوگل پلی کشف کردند که توسط بیش از ۴.۶ میلیون کاربر اندرویدی در سراسر جهان نصب شده‌اند.

بسیاری از برنامه‌های مخرب کلاهبرداری در تبلیغات هستند که با استفاده از همان کد مشترک موسوم به "Soraka " با نام پکیج (com.android.sorakalibrary. *) استفاده می‌کنند.

"GBHackers on Security" چندین گزارش را درخصوص تبلیغات مخرب در چند ماه گذشته منتشر کرده است که به سرعت در حال رشد هستند که کاربران اندرویدی را به‌طور انحصاری هدف قرار دهند تا میلیون‌ها دلار درآمد کسب کنند.

بدافزارهای مخرب، جاسوس افزارها و تبلیغ‌افزارها می‌توانند با آن دسته همراه شده و سیستم‌های کاربر را آلوده کرده و منجر به اختلال در روند روتین و نشت اطلاعات شخصی دستگاه‌های اندرویدی شوند.

علاوه بر پکیج کد Soraka، محققان همچنین در برخی از برنامه‌ها نوعی کد با عملکرد مشابه را کشف کردند که آن را "soga" با نام پکیج (com.android.sogolibrary) لقب داده‌اند.

برخی از فعالیت‌های اپلیکیشن‌های مخرب:

یک اپلیکیشن به نام "best fortune explorer app" که توسط JavierGentry80 منتشر شده است، اقدام به انواعی از فعالیت‌های مخرب از جمله فریب کاربران برای کلیک بر روی تبلیغات جهت درآمدزایی،کرده است. این برنامه‌ها دارای بیش از ۱۷۰۰۰۰ نصب بدون شناسایی توسط VirusTotal بوده است. قبل از انتشار تبلیغات جعلی، این تبلیغ‌افزارها موارد مختلف کنترلی و چک کردن کد را دور می‌زند، از جمله کدهای:

- Screen On
- TopActivity
- Interval since installation
- Trigger on/off switches
- Ad Network daily count limit
- Trigger time interval (to space out the ad rendering for each trigger)

مکانیسم و روش‌های مبهم‌سازی به مهاجمان کمک می‌کند تا از تجزیه و تحلیل خودکار بدافزارشان جلوگیری کنند. در فعالیت‌های مربوط به کلاهبرداری در تبلیغات، با باز کردن قفل دستگاه، در حالی که صفحه تلفن خاموش است کد برنامه، سرویس اعلان پس‌زمینه را که تمام فعالیت‌های کلاهبرداری را متوقف می‌کند، حذف می‌کند و اولین آگهی Out-of-Context (OOC) چند ثانیه بعد از باز کردن قفل گوشی ارائه داده می‌شود.

مهاجمان از سازوکارهای ماندگاری مبتنی بر کد جاوا برای حفظ بدافزار در دستگاه آلوده اندرویدی استفاده می‌کنند.

"این مکانیسم همچنین اجازه می‌دهد تا با استفاده از کنترل سیستم‌عامل‌ها ، افرادی که تبلیغات مخرب را دریافت می‌کنند، کنترل کنند و وقتی شرایط این امر مناسب است، برنامه‌ها تبلیغات خارج از زمینه ارائه می‌دهند" .

تیم اطلاعاتی White Ops Threat گفته‌اند که آن‌ها همچنان نظارت بر این پکیج‌ها را دارند و هرگونه پکیج‌های در حال ظهور مبتنی بر موارد قبلی را شناسایی می‌کنند.

در ادامه اسامی پکیج‌های آلوده آمده است که اگر کاربری این پکیج‌ها را نصب کرده است توصیه می‌شود آن را حذف نماید.

نام پکیج‌ها:

art.photo.editor.best.hot

bedtime.reminder.lite.sleep

com.am.i.the.best.friends.hh

com.appodeal.test

com.beauty.mirror.lite

com.bedtimehelper.android

com.bkkmaster.android

com.calculator.game

com.card.life

com.cartoon.camera.pro.android

com.code.identifier.android

com.code.recognizer.android

com.color.spy.game

com.cute.kittens.puzzlegame.android

com.cute.love.test.android

com.daily.wonderfull.moment

com.dailycostmaster.android

com.dangerous.writing.note

com.data.securite.data

com.days.daysmatter365.android

com.days.remind.calendar

com.detector.noise.tool

com.dodge.emoji.game

com.dog.bark.picture.puzzle

com.drink.water.remind.you

com.ezzz.fan.sleep.noise

com.fake.call.girlfriend.prank2019

com.fakecaller.android

com.fake.caller.plus

com.false.location

com.fancy.lovetest.android

com.fast.code.scanner.nmd

com.filemanagerkilopro.android

com.filemanagerupro.android

com.filemanageryo.android

com.filemanagerzeropro.android

com.find.difference.detective.little

com.find.you.lover.test

com.frame.easy.phone

com.frank.video.call.lite

com.free.code.scanner.nmd

com.free.lucky.prediction.test

com.funny.lie.truth.detector

com.funny.word.game.english

com.game.color.hunter

com.ice.survival.berg

com.idays.dayscounter.android

com.important.days.matter

com.instanomo.android

com.isleep.cycleclock.android

com.led.color.light.rolling

com.lite.fake.gps.location

com.lovetest.plus.android

com.love.yourself.women

com.lucky.charm.text

com.lucky.destiny.teller

com.magnifying.glass.tool

com.math.braingame.puzzle.riddle

com.math.iq.puzzle.riddle.braingame

com.math.puzzles.riddle.braingame

com.multiple.scanner.plus.nmd

com.my.big.days.counter

com.my.constellation.love.work

com.my.pocker.mobile.mirror

com.nanny.tool.data

com.nice.mobile.mirror.hd

com.nomophotoeditor.android

com.non.stop.writing

com.phone.lite.frame

com.phone.mirror.pro

com.pocker.pro.mobile.mirror

com.prank.call.fake.ring

com.phonecallmaker.android

com.pro.test.noise

com.puzzle.cute.dog.android

com.scan.code.tool

com.simple.days.counter

com.sleep.comfortable.sounds

com.sleep.in.rain

com.sleepassistantool.android

com.sleeptimer.android

com.smart.scanner.master.nmd

com.test.find.your.love

com.test.fortune.tester

com.test.lover.match

com.tiny.scanner.tool.nmd

com.wmmaster.android

com.word.fun.level.english

good.lucky.is.coming.hh

mobi.clock.android

my.lucky.goddness.today.test

newest.android.fake.location.changer

nmd.andriod.better.calculator.plus

nmd.andriod.mobile.calculator.master

nmd.android.best.fortune.explorer

nmd.android.better.fortune.signs

nmd.android.clam.white.noise

nmd.android.fake.incoming.call

nmd.android.good.luck.everyday

nmd.android.location.faker.master

nmd.android.multiple.fortune.test

nmd.android.scanner.master.plus

nmd.android.test.what.suitable

photo.editor.pro.magic

pic.art.photo.studio.picture

relax.ezzz.sleep.cradle

super.lucky.magican.newest

test.you.romantic.quize

well.sleep.guard.relax

your.best.lucky.master.test.new

com.ssdk.test

bedtime.reminder.lite.sleep

com.frank.video.call.lite.pro.prank

com.personal.fortune.text

com.daily.best.suit.you

com.false.call.trick

منبع:

/https://gbhackers.com/100-malicious-apps-from-google-play