بسمه‌تعالی

گزارش کامل بررسی اپلیکیشن‌های اینستاگرامی مارکت‌های ایرانی

بخش سوم: برنامه‌های منتشر شده در Google Play

فهرست مطالب

۱ چکیده

در قسمت‌های قبلی این مجموعه گزارش، برنامه‌های سارق در مارکت‌های ایرانی و برنامه‌های استخراج کننده پسورد بررسی شدند. در ادامه بررسی این برنامه‌ها، وجود برنامه‌ها در گوگل‌پلی بررسی شده و برای اطمینان، نسخه‌های موجود در گوگل‌پلی دوباره بررسی شدند. طبق این بررسی‌ها اقلا یک برنامه سارق (با نام بسته ir.smartmob.followergram) با حداقل ده هزار نصب که صفحه جعلی به کاربران نشان می‌دهد در گوگل‌پلی یافت شد.

همچنین بسیاری از برنامه‌های دیگر نیز باوجود اینکه به کاربر اطمینان می‌دادند که به رمز عبور آن‌ها دسترسی ندارند ولی با استفاده از روش‌های برنامه‌های سارق، رمز عبور کاربران را استخراج می‌کردند. برای این دسته از برنامه‌ها شواهدی از ارسال رمز عبور به سرور خود برنامه‌ها مشاهده نشد و به همین دلیل این برنامه‌ها در لیست برنامه‌های سارق ذکر نشده‌اند و در این گزارش نام آن‌ها «برنامه‌های استخراج‌کننده» نامیده شده‌اند. لیست برنامه‌های استخراج کننده که در گوگل‌پلی بودند نیز در این گزارش آورده شده است.

لازم به ذکر است که فقط برنامه‌هایی که قبلا از مارکت‌های ایرانی استخراج شده بودند بررسی شدند و تحقیق جامع دیگری بر روی برنامه‌های منتشر شده در گوگل‌پلی انجام نشده‌است.

۲ برنامه‌های منتشرشده در گوگل پلی

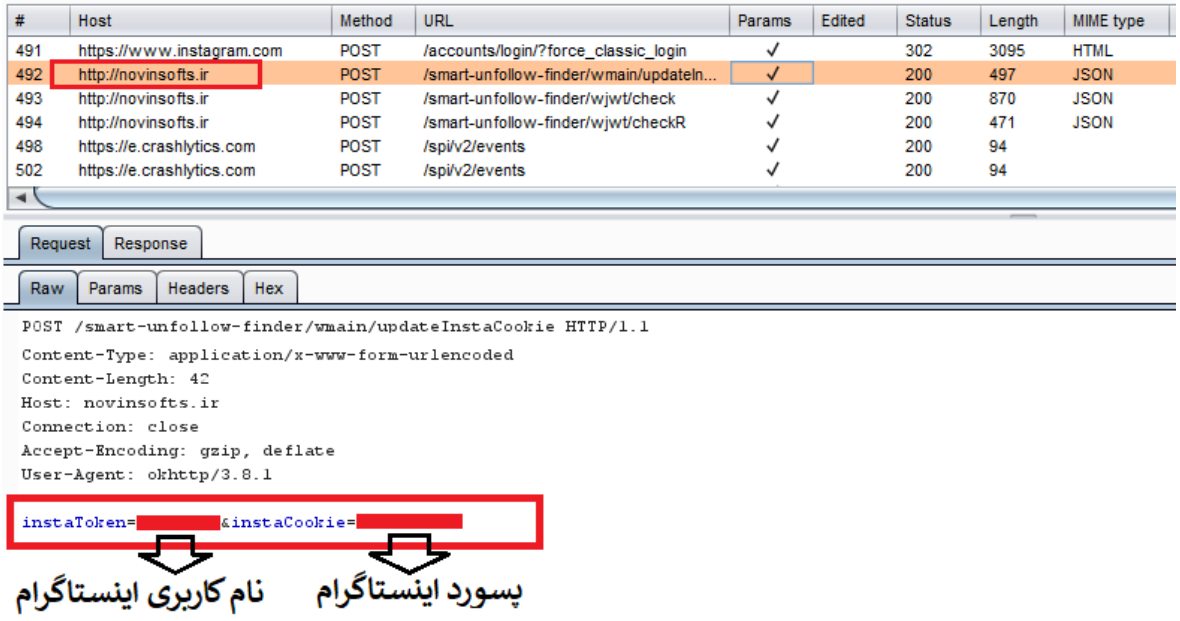
دو برنامه از بین لیست بیش از ۵۰ برنامه‌ای که قبلا ذکر شده بود در google play نیز منتشر شده‌اند، این دو برنامه از google play بررسی شدند که در ادامه اطلاعات و تحلیل مربوطه ذکر می‌شود.

۲-۱ برنامه انفالویاب اینستاگرام

اطلاعات کلی برنامه:

- نام برنامه: انفالویاب اینستاگرام
- نام بسته: com.ns.unfollowfinder
- تعداد نصب گوگل پلی: ۱۰۰۰۰+
- لینک گوگل پلی: https://play.google.com/store/apps/details?id=com.ns.unfollowfinder

نسخه‌ای از این برنامه که در مارکت‌های ایرانی منتشر شده است طبق بررسی‌ها نام کاربری و رمزعبور اینستاگرام را به سایت novinsofts.ir ارسال می‌کند. تصویری از ترافیک این برنامه که مربوط به ارسال نام کاربری و رمزعبور به سایت مربوطه است در زیر آمده است.



شکل ۱ ارسال رمز عبور اینستاگرام به novinsofts.ir

اما طبق بررسی‌ها ظاهرا نسخه گوگل پلی این برنامه در این مورد با نسخه کافه بازاری متفاوت است و شواهدی مبنی بر ارسال اطلاعات به سرور دیگر در آن یافت نشد.

۲-۲ برنامه فالوئربگیر اینستاگرام

اطلاعات کلی برنامه:

- نام برنامه: فالوئربگیر اینستاگرام
- نام بسته: ir.smartmob.followergram
- تعداد نصب کافه‌بازار: ۱۰۰۰۰+
- تعداد نصب گوگل پلی: ۱۰۰۰۰+
- لینک گوگل پلی: https://play.google.com/store/apps/details?id=ir.smartmob.followergram
- لینک google cache از صفحه گوگل‌پلی برنامه:

http://webcache.googleusercontent.com/search?q=cache:https://play.google.com/store/apps/details?id=ir.smartmob.followergram

رفتار نسخه گوگل پلی و نسخه مربوط به مارکت‌های داخلی این برنامه مشابه هم بوده و در هر دو رمز عبور کاربر به سرقت می‌رود. در هر دو نسخه این برنامه **به جای صفحه ورود به اینستاگرام یک صفحه جعلی نمایش داده می‌شود**. آدرس صفحه جعلی مربوطه http://mmbers.ir/FollowerGramNew/Instagram-Login/ است. تصویر زیر مربوط به تحلیل ترافیک برنامه است و در آن نام کاربری اینستاگرام و رمز عبور به http://mmbers.ir ارسال می‌شود.

شکل ۲ ارسال رمز عبور اینستاگرام به mmbers.ir

۳-۲ برنامه‌های استخراج کننده پسورد

لیست برنامه‌های استخراج کننده پسورد در گوگل پلی نیز بررسی شدند و طبق بررسی‌ها برنامه‌های زیر پسورد کاربران را با افزودن کد جاوااسکریپت استخراج می‌کردند، برخی از آن‌ها پسورد را به صورت آشکار نیز ذخیره می‌کنند. هرچند شواهدی از سرقت پسورد و ارسال آن به سروری به جز سرور اینستاگرام توسط این برنامه‌ها یافت نشد ولی این برنامه‌ها به صورت بالقوه خطرناک هستند و با یک آپدیت ساده برنامه توسط توسعه دهنده، امکان سرقت پسورد وجود خواهد داشت.

نام برنامه	نام بسته	نصب	توسعه دهنده	لینک گوگل پلی
انفالویاب اینستاگرام	com.ns.unfollowfinder	100	novinsofts	https://play.google.com/store/apps/details?id=com.ns.unfollowfinder
آنفالویاب اینستاگرام	com.instafollow.applex	100000	AppLex	https://play.google.com/store/apps/details?id=com.instafollow.applex

https://play.google.com/store/apps/details?id=com.MOHSEN007485.InstaFalower	Mahdi Ahmadi	100	com.MOHSEN007485.InstaFalower	فالور بگیر اینستا(اینستام مبر)
https://play.google.com/store/apps/details?id=com.pishroid.checkunfollowers	Mehrnaz Kimiyazadeh	10000	com.pishroid.checkunfollowers	آنفالویاب اینستاگرام
https://play.google.com/store/apps/details?id=ir.followertops.mohammad	Mohammad Karimi	1000	ir.follwertops.mohammad	follower and like
https://play.google.com/store/apps/details?id=com.androidineh.instacomment	neopay	5000	com.androidineh.instacomment	لایک کده- افزایش لایک اینستاگرام

۳ نتیجه‌گیری

بررسی برنامه‌هایی از مارکت‌های ایرانی که در گوگل‌پلی هم منتشر شده‌اند نشان می‌دهد که برخی از برنامه‌های خطرناک در گوگل‌پلی هم حضور دارند و حداقل یک برنامه که قطعا اطلاعات کاربران را به سرقت می‌برد در گوگل‌پلی نیز منتشر شده است.