

شناسایی برنامه‌های جدید سارق اطلاعات بانکی در فروشگاه آنلاین گوگل

بررسی‌های مؤسسه امنیتی ترندمیکرو نشان می‌دهد تعداد بدافزارهای مخفی شده در برنامه‌های موجود در فروشگاه آنلاین گوگل به منظور خالی کردن حساب‌های بانکی افزایش یافته است. این بدافزارها اطلاعات شخصی کاربران را از حساب‌های آنها جمع‌آوری کرده و تلاش می‌کنند موجودی هر حساب را خالی کنند.

از جمله اطلاعاتی که بدین شیوه سرقت می‌شود می‌توان به شماره‌های پین، شماره حساب و نام کاربری و کلمه عبور آن و غیره اشاره کرد.

این بدافزارها همچنین می‌توانند پیام‌های متنی را رهگیری کرده و گوشی‌های آلوده را تسخیر کنند. برنامه‌هایی که به مخفی کردن بدافزارها کمک می‌کنند تا آنها از سیستم امنیتی فروشگاه گوگل پلی عبور کنند، برنامه‌های دراپر نامیده می‌شوند. این برنامه‌ها دارای یک محموله متشکل از برنامه‌های مخرب هستند که گوشی‌ها را آلوده می‌کنند. بر اساس بررسی‌های ترندمیکرو، هکرها امسال به طور مخفیانه تعداد فزاینده‌ای از تروجان‌های بانکی را به فروشگاه گوگل پلی اضافه کرده اند و ظاهراً روش‌های فرار از شناسایی در این محیط مؤثر بوده است.

فهرستی از مهم‌ترین و خطرناک‌ترین این برنامه‌ها که توسط ترندمیکرو تهیه شده، به شرح زیر است:

Call Recorder APK (com.caduta.aisevsk)

Rooster VPN (com.vpntool.androidweb)

Super Cleaner- hyper & smart (com.j2ca.callrecorder)

Document Scanner - PDF Creator (com.codeword.docscann)

Universal Saver Pro (com.virtualapps.universalsaver)

Eagle photo editor (com.techmediapro.photoediting)

Call recorder pro+ (com.chestudio.callrecorder)

Extra Cleaner (com.casualplay.leadbro)

Crypto Utils (com.utilsmycrypto.mainer)

FixCleaner (com.cleaner.fixgate)

Just In: Video Motion (com.olivia.openpuremind)

Lucky Cleaner (com.luckyg.cleaner)

Simpli Cleaner (com.scando.qukscanner)

علازغم تصور عموم بر سالم بودن نرم افزار های دانلود شده از Google Play این نرم افزارها توانسته اند با دور زدن مکانیزم های امنیتی این فروشگاه اینترنتی، راه خود را به تلفن های همراه هوشمند کاربران باز نمایند. برای مقابله با این بد افزار ها راهکار های زیر پیشنهاد میگردد:

نصب آنتی ویروس روی گوشی هوشمند

حذف نرم افزارهای کم کاربرد

در صورت امکان استفاده از سامانه های تحت وب این نرم افزار ها

ارجاع به منبع خبر:

<https://www.mehrnews.com/news/5552037>