بدافزار حذف‌نشدنی Android Xhelper حتی پس از بازگردانی به تظیمات کارخانه، مجدداً خود را نصب می‌کند.

خلاصه‌ی خبر:

بدافزار Android Xhelper برای اولین بار در اکتبر ۲۰۱۹ شناسایی شد. این بدافزار که در ابتدا بصورت کاذب و نادرست به‌عنوان یک اپلیکیشن ضدویروس و تقویت‌کننده‌ی سرعت، معرفی و توزیع شده است، به‌شدت ماندگار و سرسخت است. طوری که نه با حذف آن از روی دستگاه، بلکه حتی با بازگردانی دستگاه به تنظیمات کارخانه نیز غیرفعال نمی‌شود. این بدافزار قابلیت افزایش مجوز دسترسی را دارد و نتیجتاً استفاده از تلفن‌هوشمندی که آلوده به این بدافزار است بسیار ناامن است. ساده‌ترین راه برای نجات از این بدافزار، reflash کردن دستگاه است.

Android XHelper که به دلیل قابلیت‌های ماندگاری آن مشهور شده است، برای اولین بار در اکتبر ۲۰۱۹ شناسایی شد.

کافی‌ست این بدافزار بر روی دستگاه نصب شود زیرا بعد از نصب، با وجود حذف آن توسط کاربر و یا حتی بازگردانی دستگاه به تنظیمات کارخانه، همچنان فعال می‌ماند.

بدافزار Android XHelper

این بدافزار توسط عاملان تهدید به عنوان یک اپلیکیشن ضدویروس و سرعت‌بخش محبوب برای تلفن‌های هوشمند توزیع شده است اما هیچ‌یک از عملکردهای ضدویروس یا سرعت بخشیدن را ندارد.

هنگامی که ضدویروس یا یک برنامه سرعت‌بخش نصب شود، به سادگی از صفحه اصلی یا از فهرست برنامه‌ها ناپدید می‌شود.

طبق مطالعات Kaspersky، پی‌لود تروجان رمزنگاری شده در *file /assets/firehelper.jar* اطلاعات مربوط به دستگاه قربانی مانند (android_id ، سازنده، مدل، نسخه‌ی سیستم عامل و غیره) را به سرور مهاجم ارسال می‌کند.

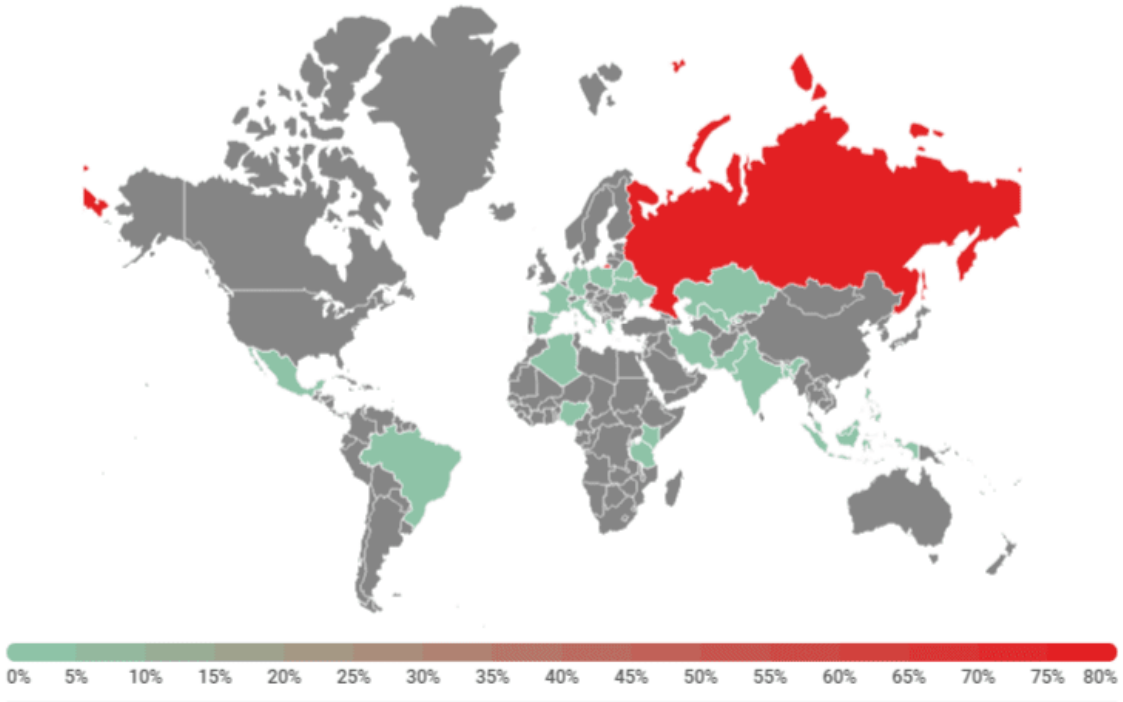
این بدافزار از روی سرور مهاجم، دومین ماژول مخرب " *Trojan-Dropper.AndroidOS.Agent.of* " را که با استفاده از کتابخانه‌ی اصلی به رمزگشایی پی‌لود می‌پردازد، بارگیری می‌کند.

dropper بعدی " *Trojan-Dropper.AndroidOS.Helper.b* " است که برای آلودگی بیشتر " *Trojan-Downloader.AndroidOS.Leech.p* " را روی دستگاه راه‌اندازی می‌کند.

Leech.p در ادامه " *HEUR: Trojan.AndroidOS.Triada.dd* " را برای افزایش سطح مجوز دسترسی در دستگاه قربانی از آن بهره‌برداری می‌کند.

در وب‌سایت نوشته شده‌است :"فایل های مخرب متعاقباً در پوشه‌ی داده‌ی برنامه ذخیره می‌شوند، که برنامه‌های دیگر به آن‌ها دسترسی ندارند. این طرح تودرتو به نویسندگان بدافزار اجازه می‌دهد تا دنباله را مخفی کرده و از ماژول‌های مخربی که برای دور زدن راه‌حل‌های امنیتی شناخته‌شده هستند، استفاده کنند. "

اگر دستگاه قربانی در حال اجرای نسخه‌های اندروید ۶ و ۷ از تولیدکنندگان چینی باشد، XHelper قادر به افزایش مجوز دسترسی و نصب مستقیم فایل‌های مخرب در پارتیشن سیستم است.



۱- تعداد کل حملات ۲۰۱۹-۲۰۲۰

این بدافزار تعدادی فایل را به پوشه‌ی *system / bin /* و تماس‌هایی را به *install-recovery.sh* اضافه می‌کند که باعث می‌شود Triada در هنگام راه‌اندازی سیستم اجرا شود.

از آنجایی که استفاده‌کردن از یک تلفن‌هوشمند آلوده به xHelper بسیار خطرناک است، ساده‌ترین روش برای پاک‌کردن این بدافزار، reflash کردن کامل تلفن است.

برخی از کاربران گفته‌اند که توانسته‌اند با خاموش‌کردن مجوزها و قفل‌کردن آن‌ها با استفاده از نرم‌افزار app lock، مانع از فعالیت‌های Xhelper شده و آن را سرکوب کرده‌اند. به گفته‌ی برخی از آن‌ها "سعی کردند مجوزهای مربوط به xHelper را بدون لغو نصب آن، رد و خاموش‌کنند اما بدافزار مجدداً همه‌ی مجوزها را فعال کرده‌است."

منبع:

https://gbhackers.com/android-xhelper-malware-2/