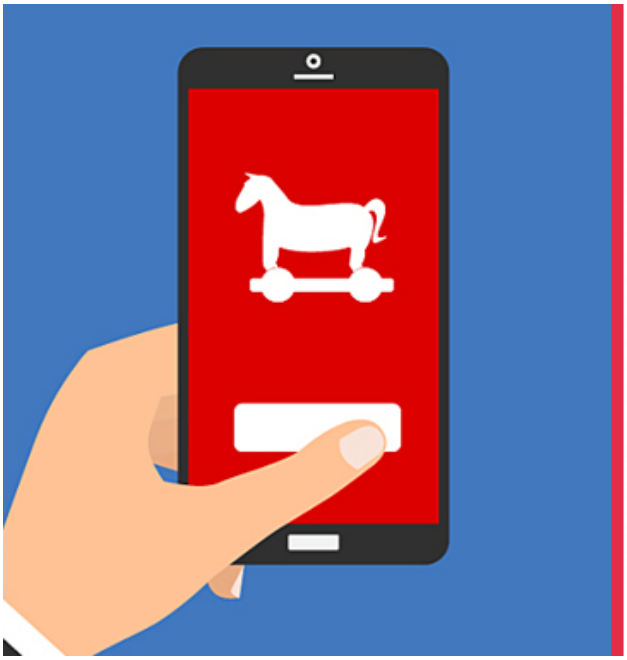
روش جدید برای نصب بدافزارهای بانکی بر روی دستگاه‌های اندرویدی توسط هکرها



خلاصه‌ی خبر:

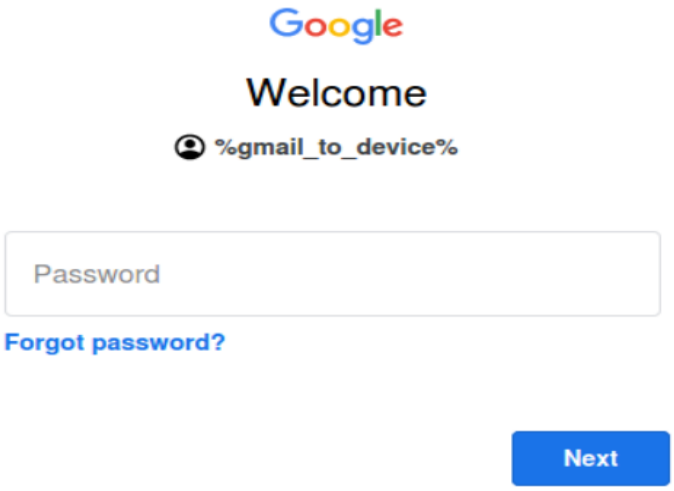
محققان امنیتی پس از مشاهده‌ی تعارضات مشابهی بر روی دستگاه‌های اندرویدی شرکت‌ها دریافتند که ۷۵٪ از سرورهای MDM(Mobile Device Manager)، برای دسترسی به دستگاه‌های اندوریدی ثبت‌شده در آن‌ها، توسط مهاجمین دور زده شده و دستگاه‌ها به نوع خطرناکی از تروجان بانکی آلوده‌شده‌اند که احتمال در دسترس قرار گرفتن اطلاعات خصوصی و حساس کاربران آن‌ها برای مهاجمین وجود دارد. این نوع مشکل تابه‌حال گزارش نشده بود ولی اکنون اهمیت آگاهی از ایمن‌سازی موبایل‌ها ضمن مدیریت آن‌ها، برای کاربران محرز و مشهود می‌باشد.

محققان امنیتی فاش کردند که هکرها حداقل ۷۵٪ از سرورهای MDM (Mobile Device Manager) را دور زده‌اند تا بدافزارهای بانکی را بطور گسترده بر روی دستگاه‌های اندرویدی نصب کنند.

MDM که با نام EMM (Enterprise Mobility Management) نیز شناخته می‌شود، ساز و کاری‌ست که عموماً توسط بسیاری از شرکت‌ها مورد استفاده قرار می‌گیرد، مانند شرکتی که با سرور ارتباط دارد تا راحت‌تر بتواند وظایفی نظیر پرداختن به تنظیمات دستگاه‌های مختلف در سراسر شرکت، مرتب‌کردن برنامه‌ها و موارد دیگر را انجام دهد.

اما، در حال حاضر این نقص اخیر ۷۵٪ از دستگاه‌های شرکت‌ها را در سراسر جهان آلوده کرده است. پس از نصب آن، این نوع خطرناک از تروجان بانکی می‌تواند مقادیر عظیمی از داده‌های حساس مانند داده‌های خصوصی کاربران، را جمع کند و به یک سرور C&C منتقل کند.

Cerberus یک تروجان بانکی است که ابتدا در ژوئن ۲۰۱۹ مشاهده شد و به صورت MaaS (Malware as a service) در دسترس است و ضمن استفاده توسط افرادی بغیر از نویسندگان بدافزار و راحتی کار برای آنها، به مهاجمان نیز اجازه می‌دهد دستگاه‌هایی را که در طول حملاتشان به خطر افتاده‌اند، پیکربندی و کنترل کنند.



۱- پاپ‌آپ HTML برای سرقت اعتبارنامه‌های کاربر Gmail

بازگردانی تنظیمات کارخانه در تمام دستگاه‌های ثبت شده

پس از دسترسی به سرور شرکت، که از نوع MDM است، هکرها استقرار برنامه را آغاز کرده و موفق به دور زدن فرایند امنیتی تقریبا ۷۵ درصد از دستگاه‌های اندرویدی شرکت‌ها شدند.

هنگامی که دو برنامه‌ی مخرب در مدت زمان کوتاهی بر روی تعداد زیادی از دستگاه‌های شرکت نصب شدند، محققان کنجکاو شدند و با کمک سرور MDM نقض‌شده، شروع به کشف این نقص کردند.

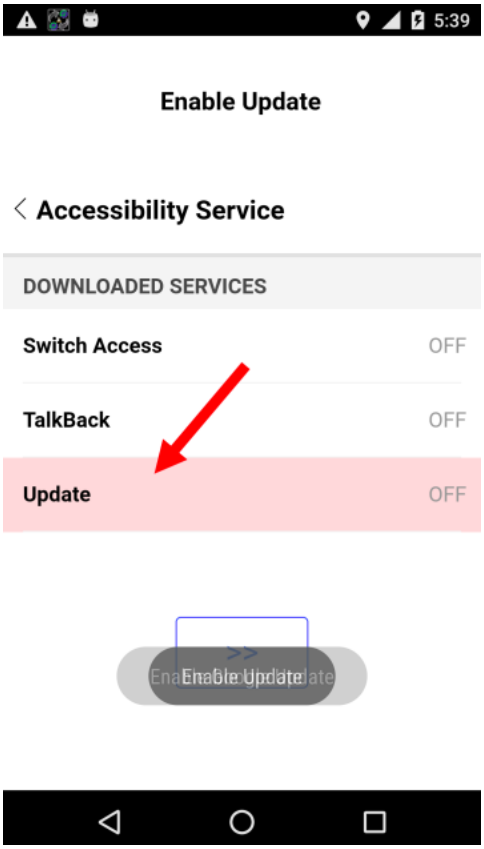
این همان چیزی است که محققان Check Point در مورد آن اظهار داشتند:"این اولین باری‌ست که ما یک رخداد گزارش‌شده در مورد توزیع بدافزارهای موبایل را منتشر می‌کنیم که از سرور MDM به عنوان یک بردار حمله استفاده می‌کند."

علاوه بر این، محققان امنیتی در Check Point به این نتیجه نیز رسیده‌اند که برای رهایی از این بدافزار و توانایی مهاجم در کنترل دستگاه‌های آلوده‌ی اندرویدی، شرکت‌ها باید بلافاصله کلیه‌ی دستگاه‌های اندرویدی ثبت شده در سرور MDM تحت‌کنترل را به تنظیمات کارخانه بازگردانند.

حفظ و تأمین دسترسی به دستگاه‌های تحت‌کنترل

Cerberus به‌سادگی با جلوگیری از تلاش قربانیان برای حذف برنامه TeamViewer در گوشی کاربران، دسترسی خود به دستگاه‌های تحت‌کنترل را تضمین می‌کند.

جدای از این، دسترسی ادمین را نیز بدست می‌آورد و به سادگی حذف هر برنامه‌ای که برای اجرای کارهای مخرب خود لازم دارد را به تعویق می‌اندازد و با بدافزار نیز به همین صورت پیش می‌رود، زیرا به سادگی همه‌ی کاربرانی را که سعی در حذف برنامه دارند، مسدود می‌کند.



۲- پنجره‌ی پاپ‌آپ که از کاربر می‌خواهد سرویس دسترسی را به‌روز کند

علاوه بر این Cerberus برای جلوگیری از شناسایی و حذف‌خودکار، سیستم امنیتی داخلی علیه بدافزار در اندروید (Google Play Protect) را بر روی دستگاه‌های اندرویدی تحت‌کنترل، به‌سادگی با بهره‌برداری از "سرویس دسترسی"، غیرفعال می‌کند.

نظر به اینکه MDM از روشی آماده و اسده برای اداره‌ی دستگاه‌ها کمک می‌گیرد، امنیت را نیز نمی‌توان نادیده گرفت. اما، این نوع مشکل برای اولین بار اتفاق افتاد و اکنون مردم لزوم مدیریت و ایمن‌سازی دستگاه‌ها را درک می‌کنند.

منبع:

https://gbhackers.com/hackers-breached-mdm-servers-to-install-android-malware/