بدافزار DressCode پس از ۱۶ ماه هنوز فعال است - دیجیاتو

یونس مرادی | یکشنبه، ۰۸ بهمن ۱۳۹۶

سال گذشته کمپانی امنیتی Check Point از کشف بدافزاری به نام DressCode خبر داد که از موبایل قربانی، یک بات نت ساخته و امکان کنترل آن را برای هکرها فراهم می کرد.

این بدافزار خود را در قالب اپلیکیشن های سالم و عمدتا کودکانه پنهان ساخته اما پس از نصب به سیستم عامل نفوذ کرده و از فعالیت های کاربر جاسوسی می کند. حتی در صورت نفوذ بیشتر بدافزار مذکور می تواند به شبکه های خصوصی کاربر نیز دسترسی پیدا کرده و اطلاعات مهم را برای خود ارسال کند.

اکنون و پس از گذشت 16 ماه از شناسایی DressCode یک هکر ثابت کرده که این بدافزار کماکان به فعالیت خود ادامه داده و تاکنون حدود 4 میلیون دستگاه را آلوده ساخته است.

آلوده شدن دستگاه های اندروید به این بدافزار بسیار خطرناک است چرا که با استفاده از پروتکل های SOCKS موبایل را مستقیما به هکرها متصل می کند. مهاجمان در ادامه می توانند به شبکه های خانگی یا اداری متصل شده و به دیگر کامپیوترها و سیستم های متصل نفوذ کنند.

این هکر اعلام کرده است که مهاجمان از سیستم های آلوده برای اجرای تبلیغات کلیکی استفاده می کنند که سود سرشاری را نصیب آنها می کند. در حال حاضر لیست جدیدی از اپلیکیشن های آلوده به این بدافزار در گوگل پلی منتشر نشده اما بسیاری از اپ های آلوده کماکان در مارکت های شخص ثالث از قبیل APKPure در دسترس قرار دارند.

سال گذشته تیم امنیت سایبری TrendLabs اعلام کرد که DressCode در بیش از 3 هزار اپلیکیشن تعبیه شده که حداقل 400 مورد از آنها در گوگل پلی منتشر شده اند. برای مثال می توان به GTA V برای بازی Minecraft: Pocket Edition اشاره کرد که در همان زمان بیش از پانصد هزار بار در گوگل پلی استور دانلود شده بود.

چند ماه قبل نیز کمپانی سیمنتک اعلام کرد که بدافزار Sockbot در قالب اپلیکیشن هایی که اسکین های مختلف را برای کارکترهای بازی ماینکرفت ارائه می دهند روی دستگاه قربانی نصب شده و آن را به بات تبدیل می سازد.

یکی از راه های معمول مقابله با این بدافزارها تحت کنترل درآوردن سرورهای اجرا کننده آنها است

که Sinkholing نام دارد، با این حال مشخص نیست گوگل در این زمینه چه گام هایی را برداشته است، با این حال ارائه این شواهد از فعالیت DressCode کارایی راهکاری گوگل برای مقابله با بدافزارهایی از این دست را زیر سوال می برد.

دیجیاتو