وقتی که ترموستات Nest هک می شود؛ سلام! من دوست دارم دمای خانه شما را افزایش دهم - دیجیاتو

مانی قاسمی | یکشنبه، ۱۹ مرداد ۱۳۹۳

شاید پیشرفت های اخیر این تصور را در شما به وجود آورده باشد که تکنولوژی «اینترنت اشیا» آماده بهره برداری است و می تواند در طول چند سال آینده با سرعت بسیاری فراگیر شود. اما بهتر است بدانید که هکر ها و متخصصین امنیتی باوری دگر دارند و هنوز راه بسیاری را برای «اینترنت اشیا» متصور هستند.

در حاشیه کنفرانس Black Hat، که در طول هفته گذشته در لاس وگاس به وقوع پیوست، تیمی تشکیل شده از چند هکر و مهندس جوان، بر روی صحنه رفت و توانست سیستم ترموستات Nest را هک نماید.

برای کسانی که با Nest آشنا نیستند باید توضیح دهیم که این دستگاه یک ترموستات هوشمند است که به شما اجازه می دهد از طریق تلفن هوشمند، دمای خانه را کنترل نمایید. Nest با استفاده از سنسورهایی که داخل خانه شما دارد، می تواند دما را مطابق میلتان تنظیم نماید. این سیستم هنگامی که شما خانه نباشید، به صورت خودکار به روی حالت صرفه جویی می رود تا بدین گونه انرژی کمتری را مصرف نماید. گوگل در اوایل سال جاری میلادی، Nest را به مبلغ ۳.۲ میلیارد دلار، خریداری کرد.

دنیل بوئنتلو، یک دانشجو و محقق امنیتی در دانشگاه فلوریدا در کنفرانس Black Hat این سؤال را مطرح کرد که آیا امنیت قربانی شده در «اینترنت اشیا»، ارزش راحتی بدست آمده را دارا است؟

دنیل توضیح می دهد که: «شما در اینجا با کامپیوتری مواجه هستید که حتی نمی توانید بر روی آن آنتی ویروس نصب کنید. این محصولات همگی راه نفوذی دارند که یک آدم خلافکار می تواند از آن ها برای ورود به خانه شما استفاده کند و همواره نیز در آنجا باقی بماند.»

اگر شما یک کامپیوتر ویروسی شده داشته باشید، با مشکلاتی که در عملکرد آن به وجود می آید، سرانجام به یک تعمیرکار مراجعه می کنید؛ اما در مورد ابزار هایی همچون Nest، قربانی هرگز نمی تواند متوجه حضور هکر در سیستم خود شود، چرا که همه چیز مانند سابق به کارکرد خود ادامه می دهد.

دنیل و تیمش، برای اینکه ضعف امنیتی Nest را به حاضرین در همایش Black Hat نشان دهند، بر روی سن یک USB را به دستگاه متصل کردند و در ظرف چند دقیقه موفق شدند کد مورد نظر خود را در برنامه دستگاه جایگزین نمایند. در این مرحله آن ها توانستند کنترل دستگاه را در دست گیرند و حتی پیغام خاصی را بر روی نمایشگر ترموستات به تصویر در آورند.

با استفاده از اطلاعات بدست آمده از طریق Nest، هکر های می توانند عادات زندگی شما را متوجه شوند و حتی زمان هایی که در خانه نیستید را نیز پیش بینی نمایند. با استفاده از این قبیل اطلاعات، مقدمات برای خلاف های دیگر نیز فراهم می شود.

در حالی که گوگل هنوز اقدام خاصی را جهت برطرف کردن ضعف امنیتی Nest انجام نداده، هکر ها مشغول بررسی روش هایی هستند تا بتوانند این ترموستات هوشمند را از راه دور نیز هک نمایند.

به نظر شما ابزارهای تکنولوژی، در آینده می توانند تهدیدی امنیتی برای کاربران به شمار روند؟

دیجیاتو