حمله باج‌افزاری به دوربین‌های CCTV

نفوذ هکرها به دوربین‌های مداربسته پلیس واشنگتن

هکرها هشت روز پیش از برگزاری مراسم تحلیف ریاست جمهوری ایالات متحده موفق شده بودند دستگاه‌های ذخیره‌ساز و دوربین‌های نظارتی که از سوی اداره پلیس واشنگتن مورد استفاده قرار می‌گیرد را هک کنند.

واشنگتن پست به تازه‌گی گزارش کرده است، تنها چند روز پیش از برگزاری مراسم تحلیف ریاست جمهوری دونالد ترامپ، هکرها موفق شده بودند دستگاه‌های ذخیره‌سازی که داده‌های متعلق به دوربین‌های مداربسته نظارتی را ضبط می‌کردند و از سوی اداره پلیس مورد استفاده قرار می‌گرفتند را هک کنند. بر اساس گزارش منتشر شده از سوی واشنگتن پست، 70 درصد از دستگاه‌های ذخیره‌سازی که به واسطه این حمله آلوده شده بودند از سطح شهر و دفاتر فناوری این شهر جمع‌آوری شدند و دستگاه‌های دیگری جایگزین آن‌ها شده است. این اتفاق دقیقا هشت روز پیش از برگزاری مراسم تحلیف ریاست جمهوری جدید ایالات متحده رخ داده بود. اما سوال این است که چه ویروسی می‌تواند به این شکل به دستگاه‌های ذخیره‌ساز ضربه بزند؟

مطلب پیشنهادی

پیاده‌سازی حمله DDoS در سراسر جهان
از دوربین‌های مدار بسته زامبی فاصله بگیرید + چگونه مشکل را حل کنیم؟

خوب، در جواب این پرسش باید بگوییم یکی از محبوب‌ترین و پر استفاده‌ترین گونه‌های بدافزاری که این روزها به دفعات مورد استفاده قرار می‌گیرد یعنی باج‌افزارها در پس این حمله قرار داشتند. این باج‌افزار به مدت سه روز و از تاریخ 12 تا 15 ژانویه به دوربین‌های اداره پلیس اجازه نداد تا فیلم‌های مربوط به این سه روز را ضبط کنند. این اتفاق باعث شده بود که شهروندان این شهر به مدت سه روز در معرض تهدیدات احتمالی قرار داشته باشند. هر چند مقامات مربوطه این حرف را رد می‌کنند. واشگنتن پست در بخشی از پست خود آورده است از 187 دوربین ویدویی که در این شهر به سامانه تلویزیونی نظارتی مداربسته متصل هستند تعداد 123 مورد به واسطه این حمله آلوده شده بودند. پلیس خود اعتراف کرده است که این تعداد دوربین به باج‌افزار فوق آلوده بوده‌اند، اما در عین حال یادآور شده است که دوربین‌های آلوده عمدتا در مناطق عمومی قرار داشته‌اند. در نتیجه این حمله هیچ‌گونه تاثیری بر

شبکه‌های کامپیوتری این شهر نداشته است.

مطلب پیشنهادی

هوش مصنوعی به‌کمک دوربین‌های نظارتی می‌آید
تشخیص سریع بسته‌های مشکوک با دوربین‌های امنیتی مجهز به AI

باجی پرداخت نشده است

به نظر می‌رسد در زمان درست کردن دستگاه‌های ذخیره‌ساز و آماده‌سازی آن‌ها برای استفاده مجدد و همچنین درست کردن دوربین‌های نظارتی، اداره پلیس هیچ‌گونه باجی را پرداخت نکرده است.

باج‌افزارها یکی از شایع‌ترین و پر استفاده‌ترین روش‌های هک هستند که این روزها به دفعات از سوی هکرها مورد استفاده قرار می‌گیرند. هکرها همواره کاربران را ترغیب می‌کنند تا روی یک لینک کلیک کرده یا ضمیمه یک ایمیل را باز کنند. ضمیمه‌هایی که عمدتا فایل‌های PDF هستند و به راحتی بدافزارها را به درون کامپیوتر قربانیان وارد می‌کنند. زمانی که باج‌افزاری به درون سیستم قربانی وارد شد بلافاصله فایل‌ها را رمزنگاری کرده و مادامی که کاربر باج مربوطه را به هکر پرداخت نکند کد دسترسی به فایل‌ها را در اختیار او قرار نمی‌دهد. هکرها به طور معمول باج را به شکل بیت‌کوین دریافت می‌کنند تا امکان ردیابی آن‌ها وجود نداشته باشد. هکرها به تازگی از این مکانیزم حمله در ارتباط با اسمارت‌فون‌ها نیز استفاده کرده‌اند هرچند مقیاس آن محدود بوده است.

هنوز به درستی مشخص نیست چه فرد یا گروهی در پشت این حمله قرار داشته است. اما متقارن شدن این حمله با تحولات اخیر باعث شده است تا کار پلیس در شناسایی عاملان این حمله سخت شود.

تاریخ انتشار:

15 بهمن 1395

نشانی منبع: https://www.shabakeh-mag.com/security/6650