هکرها با بهره‌مندی از کد مخرب NSA موفق شدند به ده‌ها هزار روتر نفوذ کنند - دیجیاتو

مانی میرجوادی | جمعه، ۰۹ آذر ۱۳۹۷

به نظر می‌رسد هکرها توانسته‌اند با استفاده از کدهای مخرب مایکروسافت -که سال گذشته پس از کش و قوس با آژانس امنیت ملی ایالات متحده به صورت عمومی در اختیار همه قرار گرفته بود- به حدود ۴۵ هزار روتر در سرتاسر دنیا نفوذ داشته باشند.

ارائه دهنده‌ی خدمات ابری و انتقال دهنده‌ی شبکه‌ای محتوا یعنی شرکت آکامای روز پنجشنبه در یک پست اعلام کرد که مهاجمینی که زیرساخت‌های آسیب پذیر UPnP را هدف قرار داده بودند موفق شده‌اند به ده‌ها هزار روتر نفوذ داشته باشند.

UPnP یک پروتکل معروف به شمار می‌رود که به دستگاه‌ها اجازه می‌دهد در یک شبکه‌ی محلی دستگاه‌های دیگر متصل شده به شبکه را شناسایی کنند. آکامای گزارش داده که از بین ۳.۵ میلیون دستگاه، حدود ۸ درصدشان از نسخه‌ی آسیب پذیر UPnP استفاده می‌کردند.

پروتکل UPnP به دفعات در گذشته نیز مورد حمله‌ی مهاجمین قرار گرفته است. عموما از طریق در معرض نمایش قرار دادن دستگاه‌هایی از اینترنت که تنها باید به صورت محلی نمایش داده شوند. آکامای گزارش داد که تابستان گذشته، UPnP توسط هکرها مورد استفاده قرار گرفت تا بتوانند ترافیک‌ها را در یک سوء استفاده‌ی هماهنگ شده و گسترده، پنهان کنند.

حمله‌ی جدید که پورت ۱۳۹ و ۴۴۵ را هدف قرار داده بود از EternalBlue استفاده می‌کرد. این کد مخرب توسط NSA ایجاد و توسعه داده شده بود اما توسط گروهی از هکرها به نام Shadow Brokers در دسترس همگان قرار گرفت. کمی بعد از این کد مخرب در چند حمله‌ی دیگر نیز استفاده شد.

دو هفته پیش، وبسایت آرس تکنیکا به صورت جزئی نشان داد که چگونه ۱۰۰ هزار بات نت روتر تولید شده است. این آلودگی عظیم توسط نت لب 360 پیدا شد.

متاسفانه محققین نتوانستند اعلام کنند که به طور دقیق چه اتفاقی برای این ۴۵ هزار روتر آلوده خواهد افتاد. اما یک حمله‌ی موفق بنابر اعلام محققین می‌تواند منجر به حمله‌ی بدافزارها و ایجاد چنین امکانی شود. همچنین احتمال ماندگاری مداوم این آلودگی در شبکه نیز وجود خواهد داشت.

دیجیاتو