ویکی‌لیکس پس از افشای رایانامه‌های حزب دموکرات آمریکا گرفتار حملات DDoS شد

فقط دو روز به انتخابات ریاست‌جمهوری آمریکا باقی مانده است، در این اوضاع ویکی‌لیکس در ساعات پایانی یکشنبه دست به انتشار گنجینه‌ی تازه‌ای از رایانامه‌ها زده که ظاهراً از کمیته‌ی ملی حزب دموکرات (DNC) به دست آورده است.

در تازه‌ترین افشاسازی وب‌گاه افشاگر ویکی‌لیکس حدود ۸۰۰۰ نسخه‌ی رونوشت از رایانامه‌های متعلق به DNC در دسترس کاربران قرار گرفته است؛ ویکی‌لیکس در مجموع ۵۰،۰۰۰ رایانامه‌ی به سرقت رفته از چهره‌ی کلیدی حزب دموکرات آمریکا، رئیس ستاد تبلیغاتی هیلاری کلینتون، جان پودستا را برملا کرده است.

با این حال، این بار همه‌چیز مطابق برنامه‌های ویکی‌لیکس پیش نرفته است. ویکی‌لیکس صبح دوشنبه در توییتر بیان داشت که کمی پس از انتشار رایانامه‌های به دست آمده از DNC، مورد آماج حملات انسداد سرویس توزیع‌شده گرفته است.

کمی پس از آن‌که ویکی‌لیکس یک حمله‌ی DDoS علیه کارگزارهای انتشار رایانامه‌اش را گزارش کرد، توییترِ این وب‌گاه هم از کار افتاد و این قطعی ۳۰ دقیقه به طول انجامید.

با توجه به شواهد، این قطعی توییتر از ساعت ۶:۴۵ قبل از ظهر آغاز و حدود نیم ساعت ادامه پیدا کرده است؛ گزارش‌ها حاکی از آن هستند که این تأثیر روی کاربران متغیر بوده است و بسیاری از کاربران در ژاپن با وجود گذشت چند ساعت باز هم از تبعات این رخداد خلاص نشده بودند.

ویکی‌لیکس در صفحه‌ی فیس‌بوک خود نوشت: «ما هنوز هم در حال تجربه‌ی یک حمله‌ی انسداد سرویس در کارگزارهای انتشار رایانامه‌ی خود هستیم، و به نظر می‌رسد که توییترمان هم از کار افتاده باشد، اما نمی‌توانیم با قطعیت نظر بدهیم که این قطعی نشانه‌ی حمله به حساب توییتر ما می‌باشد.»

ویکی‌لیکس در دسترس نیست، توییتر در دسترس نیست، چه ارتباطی میان این دو حادثه است؟

در این لحظه هیچ ارتباطی میان این دو رخداد وجود ندارد، هرچند برخی از کاربران توییتر به سرعت این دو واقعه را به هم ربط داده‌اند.

نتیجه‌ی انتخابات ریاست‌جمهوری آمریکا، خبری ناخوشایند برای اپل و مایکروسافت

اگرچه عده‌ی اندکی از شهروندان آمریکایی انتظار این نتیجه را داشتند، اما با اتمام انتخابات باید دونالد ترامپ را به عنوان رئیس‌جمهور جدید خود بپذیرند؛ حال جمعیت کثیر کارکنانی که در حوزه‌ی فن‌آوری این کشور فعالیت می‌کنند می‌بایست طی چهار سال آینده شاهد تغییر ارتباط دولت جدید با شرکت‌های عظیم فنی باشند.

متأسفانه خبر انتخاب ترامپ برای سیلیکون ولی اصلا خوشایند نیست، بیشتر به این خاطر که این جمهوری‌خواه بارها و بارها شرکت‌های عرصه‌ی فن‌آوری مانند اپل (به خاطر آیفون) را به جهت ساخت محصول در خارج از مرزهای این کشور مورد انتقاد قرار داده است.

حماسه‌ی سن برناردینو

علاوه بر این، ترامپ اغلب موارد مشابه با اپل و مایکروسافت را به خاطر این‌که در فقره‌های بحث‌برانگیز مانند آیفونِ حادثه‌ی سن‌برناردینو تحت قوانین آمریکا فعالیت نمی‌کنند، محکوم کرده است؛ همان‌طور که در خبرها گفتیم، در این حادثه FBI از اپل خواسته بود تا به تلفن یکی از تیراندازان دسامبر ۲۰۱۵ پیدا کند. اگرچه اپل به شدت با این درخواست مخالفت کرد و متعهد شد که حریم خصوصی بی‌عیب و نقصی را به کاربران خود ارائه کند، و به هویت آن‌ها کاری نداشته باشد، اما برخی از مقامات رسمی این شرکت را مورد بمباران سرزنش‌های خود قرار دادند، این مقامات می‌گویند که اپل امنیت ملی را زیر سؤال برده و از تروریست حمایت می‌کند.

بدیهی است که ترامپ یکی از همین منتقدان بوده، وی با کلمات بسیار تند و تیزی ادعا می‌کرد که اگر در مقام ریاست‌جمهوری بود هرگز اجازه نمی‌داد اپل دست به چنین کاری بزند.

ترامپ می‌گفت: «فکر می‌کنید آن‌ها چه کسی هستند؟ شما باید قفل این گوشی را باز کنید. من به‌طور کلی به امنیت فکر می‌کنم، ما باید این قفل را باز کنیم، ما باید از مغزمان استفاده کنیم؛ ما باید عقل سلیمان را به کار بیاندازیم!»

با این حال که ترامپ صاحب سهام چند میلیون دلاری اپل است، اما این موضوع باعث نشده که وی از درخواست تحریم محصولات تولیدی توسط این شرکت مطرح و محبوب دست بردارد.

تروریست‌های داعشی شما را می‌بینند

یک شرکت امنیتی آمریکایی با نام (BLACKOPS Cyber(BOC می‌گوید تهدیدی جدید را در ماه اکتبر کشف کرده است که نشان می‌دهد تروریست‌ها اخیراً بر روی توسعه منابع فنی تمرکز داشته‌اند.

BOCطی گزارشی به مقامات اعلام کرده است موفق شده یک گروهک معروف داعشی را شناسایی کند که آسیب‌پذیری‌های مختلف سامانه‌های نظارتی را به همراه نوع دسترسی به این سامانه‌ها به‌صورت عمومی منتشر می‌کرده است. در این گزارش شواهدی ارائه شده است مبنی بر این‌که از اواخر تابستان و اوایل پاییز دو گروه داعشی آدرس دوربین‌های امنیتی را منتشر می‌کرده‌اند. این دوربین‌ها در مناطق مختلفی از آمریکا و اروپا گرفته تا آسیا و آمریکای لاتین بوده‌اند. در کنار فهرست این دوربین‌ها، تروریست‌های داعشی ویدئویی نیز منتشر کرده‌اند که چگونگی دسترسی به دوربین‌های مذکور را نشان می‌داده است. یکی از متخصصان امنیتی BOC که ویدئوهای مربوطه را بررسی کرده است می‌گوید: «آسیب‌پذیری موجود یک آسیب‌پذیری روت‌کیت بوده که بهره‌برداری از آن نیاز به دانش فنی زیادی ندارد.»

BOC می‌گوید لازم است شرکت‌های نظارتی ویدئویی آسیب‌پذیری‌های امنیتی خود را کشف کرده و آن‌ها را هرچه سریع‌تر برطرف سازند. حملات اخیر علیه ارائه‌دهنده خدمات DNS با نام Dyn که با بهره‌گیری از باتنت‌های IoT انجام شد اهمیت تأمین امنیت را در دستگاه‌هایی مانند CCTV و DVR های متصل به اینترنت نشان می‌دهد.

کارشناسان BOC می‌گویند نگرانی اصلی آن‌ها این است که تروریست‌های داعشی از کنترل این دوربین‌ها برای مخفی‌کردن عملیات‌های مختلف خود استفاده کنند. البته نگرانی دیگر به استفاده از این دوربین‌های در حملات مختلف نظیر آنچه برای Dyn اتفاق افتاد مربوط می‌شود. «می‌دانیم که تروریست‌های داعشی پیش از انجام حمله به‌دقت محل موردنظر خود را بررسی می‌کنند، این امکان جدید می‌تواند در انجام حملات به‌شدت به آن‌ها کمک کند.» در گزارش BOC آمده است: «انجام حملات به شکل ساده‌تر همان هدفی که به نظر می‌رسد گروهک تروریستی داعش می‌خواهد با استفاده از فناوری به آن دست یابد.

مقامات آمریکایی می‌گویند آماده مقابله با حمله احتمالی روسیه به انتخابات ریاست جمهوری هستند

برای نخستین بار، در تلافی به پویش‌های نفوذی که در طی چند ماه اخیر سیاست‌مداران مختلف آمریکایی هدف قرار گرفته‌اند یکی از مقامات دفتر ریاست جمهوری آمریکا کشور دیگری را تهدید به حمله سایبری کرده است. دفتر سازمان اطلاعات ملی و سازمان امنیت داخلی به اتفاق بیانیه‌ای امنیتی را منتشر کردند که طی آن دولت روسیه متهم شده است. در این بیانیه دولت روسیه مقصر اصلی نفوذهای اخیر به سازمان‌های ایالتی آمریکایی معرفی شده است که درگیر انتخابات ریاست جمهوری این کشور هستند.

در این بیانیه آمده است: «USIC اطمینان دارد که دولت روسیه سوءاستفاده‌های اخیر از رایانامه‌های افراد و سازمان‌های مختلف آمریکایی از جمله سازمان‌های سیاسی را مدیریت می‌کرده است. بررسی رایانامه‌های مورد نفوذ واقع‌شده و منتشرشده در وبگاه‌هایی مانند DCLeaks.com و ویکی‌لیکس شواهدی را مبنی بر شباهت این حملات با روش‌هایی که روسیه استفاده می‌کند، نشان داده است. این سرقت‌ها و نفوذها در نظر دارند در روند انتخابات آمریکا تداخل ایجاد کنند.» دو هفته پیش، معاون رئیس‌جمهور آمریکا، جو بایدن طی یک مصاحبه با شبکه خبری NBC گفته بود: «پیامی درباره حملات مذکور به ولادمیر پوتین داده خواهد شد.»

به گزارش NBC، سازمان CIAدر حال آماده‌سازی حمله‌ی سایبری تلافی‌جویانه است تا به مقابله با کرملین بپردازد.

درحالی‌که متخصصان امنیتی، سیاست‌مداران و مقامات ارتش درباره نحوه پاسخ مناسب به مداخلات روسیه فکر می‌کنند، افسر ارشد سازمان اطلاعات ملی با استناد به اسناد فوق محرمانه می‌گوید ارتش سایبری ایالات متحده قبلاً به شبکه توزیع برق، شبکه ارتباطی و سامانه‌های فرمان روسی نفوذ کرده است.

روسیه، چین، آمریکا، آلمان و تقریباً تمام کشورها در حال تقویت توانایی‌های سایبری خود هستند. این روند تا جایی پیش رفته است که متخصصان امنیتی اصطلاح نظامی کردن فضای سایبری را برای آن استفاده کرده‌اند. این اصطلاح به معنای تلاش دولت‌ها به‌منظور دستیابی به‌نوعی سلطه در استفاده از بدافزارها و ابزارهای نفوذ علیه زیرساخت‌های حیاتی و سامانه‌های رایانه‌ای سایر کشورها است. مثال‌هایی همچون استاکس‌نت میزان تأثیر اسلحه‌های دیجیتال را در دنیای امروز نشان داده‌اند.