فرهیختگان

@farhikhtegandaily

WWW.FDN.IR

در یک حمله سایبری پیچیده، اطلاعات وزارت خزانه‌داری آمریکا و یک سازمان آمریکایی به سرقت رفت

آماده باش!

فرهیختگان چند روز پس از اینکه یکی از بزرگ‌ترین شرکت‌های فعال در حوزه امنیت سایبری، هدف یکی از پیچیده‌ترین حملات سایبری قرار گرفت، رسانه‌های غربی گزارش دادند وزارت خزانه‌داری آمریکا نیز هدف حملات سایبری قرار گرفته است. رویترز نخستین رسانه‌ای که این خبر را منتشر کرد از نقش «یک دولت خارجی» در این حمله خبر داد و نوشت که در جریان این حمله اطلاعات وزارت خزانه‌داری آمریکا و یک سازمان آمریکایی مسئول درباره تصمیم‌گیری درخصوص سیاست‌های اینترنت و ارتباطات، به سرقت رفته است. ۳ روز پیش از حمله روز یکشنبه به وزارت خزانه‌داری آمریکا، شرکت امنیت سایبری «فایرآی» از یک حمله «بسیار پیچیده با حمایت دولتی» خبر داد. آن‌طور که کوین ماندیا، مدیرعامل شرکت گفته بود، هدف اصلی مهاجمان به دست آوردن اطلاعات مربوط به مشتریان دولتی مشخص بوده اما موفق شدند، ابزاری که مورد استفاده برای سنجش امنیت کاربران بوده را سرقت کنند. آن‌گونه که جو تایدی، گزارشگر فضای مجازی «بی‌بی‌سی» نوشته اهمیت این حمله از آن جهت بود که برخلاف بسیاری از حملات دیگر، این بار محافظان امنیت سایبری خود هدف حمله هکرها قرار گرفته‌اند. در جریان این حمله هکرها موفق شدند اطلاعات و ابزار «تیم قرمز» شرکت فایرآی که ابزاری تهاجمی (آفندی) برای حملات آزمایشی با هدف سنجش قدرت دفاعی شبکه شرکت‌هاست را سرقت کنند. سرقت این ابزار، به معنای در اختیار گرفتن توان تهاجمی آن از سوی هکرهاست. هنوز مشخص نیست که در جریان این حمله که رسانه‌های آمریکایی آن را «بزرگ‌ترین» و «پیچیده‌ترین» عملیات سایبری در ۵ سال اخیر می‌خوانند، از ابزار «تیم قرمز» استفاده شده است یا نه ولی تا این لحظه هک شدن اطلاعات وزارت خزانه‌داری و یکی از آژانس‌های وزارت بازرگانی آمریکا تایید شده است.

پس از انتشار خبر رویترز درباره حمله سایبری، دولت ترامپ روز یکشنبه اذعان کرد هکرهایی به نمایندگی از یک دولت خارجی به شماری از شبکه‌های اصلی دولت ازجمله در وزارت خزانه‌داری و بازرگانی نفوذ کرده و به سیستم‌های ایمیل آنها دسترسی پیدا کرده‌اند. برخی از منابع از هدف قرار گرفتن آژانس‌های مرتبط با امنیت ملی خبر داده‌اند. رسانه‌ها گزارش داده‌اند این حمله سایبری باعث شد تا دولت آمریکا در حالت آماده‌باش قرار بگیرد و نشست اضطراری شورای امنیت ملی در کاخ سفید برگزار شود. سازمان‌های اطلاعاتی آمریکا نگران هستند هکرهایی که وزارت خزانه‌داری آمریکا را هدف قرار داده‌اند ممکن است از ابزار مشابه برای نفوذ به دیگر سازمان‌های آمریکایی استفاده کرده باشند. وزارت خزانه‌داری آمریکا هرگونه اظهارنظر در این‌باره را به شورای امنیت ملی واگذار کرده است و شورای امنیت ملی و آژانس امنیت سایبری وزارت امنیت داخلی آمریکا نیز درحال بررسی این عملیات گسترده هستند. متخصصان، قربانیان عملیات مذکور را دولت و بخش خصوصی اعلام کردند. انگیزه انجام این حمله و نیز میزان آسیب‌های ناشی از آن همچنان نامشخص است اما به گفته چند مقام آگاه، حملات از اوایل بهار امسال درحال انجام بوده است. روزنامه نیویورک‌تایمز این حمله را یکی از پیچیده‌ترین و شاید بزرگ‌ترین حمله سایبری طی پنج سال گذشته دانست.

اتهام‌زنی علیه روسیه

گمانه‌زنی‌ها درباره دولت خارجی که گفته می‌شود در پس این حمله سایبری قرار داشته، از دقایق نخست در جریان بود. روزنامه واشنگتن‌پست دیروز گزارش کرد این حمله سایبری توسط هکرهای دولت روسیه انجام شده است. واشنگتن‌پست به نقل از یک منبع آگاه گزارش داد، پلیس فدرال آمریکا درحال بررسی کمپین یک گروه هکری است که در سرویس اطلاعات خارجی روسیه کار می‌کند و در میان شرکت‌های امنیتی بخش خصوصی به گروه ATP۲۹ یا Cozy bear معروف است. واشنگتن‌پست ادعا کرد که این گروه هکری کاخ سفید و وزارت خارجه آمریکا را نیز در دولت «باراک اوباما» هک کرده بود. هرچند این ادعای واشنگتن‌پست هنوز تایید نشده است اما با توجه به گزارش‌های مرکز مطالعات استراتژیک و بین‌المللی (CSIS)، چین و روسیه دو کشور فعال در حوزه حملات سایبری هستند. از سال ۲۰۰۶ تا ۲۰۱۸، چین در ۱۰۸ حادثه سایبری که هرکدام بیش از یک میلیون دلار ضرر داشته است، نقش داشته است. روسیه نیز از سال ۲۰۰۶ با خسارات بیش از یک میلیون دلار مسئول ۹۸ حادثه سایبری بزرگ بوده است. با این حال اما سفارت روسیه در واشنگتن ادعای دست داشتن این کشور در حمله سایبری به خزانه‌داری آمریکا را رد کرد.

زیرساخت‌های آسیب‌پذیر آمریکا

در سال‌های اخیر با توجه به گسترش فضای مجازی، تقریبا تمام زیرساخت‌های کشورهای توسعه‌یافته به اینترنت وابستگی پیدا کرده و همین وابستگی نیز به هکرها برای حملات سایبری کمک کرده است. آمریکا در سال‌های گذشته برای رفع این محدودیت، از فناوری نسبتا پیشرفته و بودجه نظامی زیادی بهره برده تا بتواند از قابلیت‌های قابل‌توجهی در دفاع از خود برخوردار باشد. آمریکا علاوه‌بر هزینه‌های سنگین در این حوزه، در سال ۲۰۱۱، استراتژی بسیار تهاجمی را در حوزه سایبری در دستور کار قرار داد. کاخ سفید برمبنای «استراتژی بین‌المللی برای فضای مجازی» اعلام کرد برای خود حق استفاده از نیروی نظامی در پاسخ به حمله سایبری را محفوظ می‌داند. با این حال اما آمریکا خود همواره علیه دشمنانش از این ابزار استفاده کرده است. ویروس «استاکس‌نت» یکی از این نمونه‌هاست. این کرم سایبری سال ۲۰۱۰ نزدیک به هزار سانتریفیوژ هسته‌ای ایران را از بین برد و براساس ادعاها، برنامه اتمی تهران را حداقل برای دو سال عقب راند. هیچ کشوری مسئولیت این حمله سایبری را برعهده نگرفت اما در اواخر ماه مه ۲۰۱۲ رسانه‌های آمریکایی اعلام کردند که استاکس‌نت مستقیما به دستور اوباما، رئیس‌جمهور آمریکا طراحی، ساخته و راه‌اندازی شده است.

پس از این حمله سایبری، ایران یک بازنگری جدی در توان سایبری خود انجام داد و توانست به یکی از قدرت‌های سایبری در جهان تبدیل شود. سایر بازیگران بین‌المللی نیز که به شکلی مورد حمله سایبری آمریکا قرار گرفته بودند، به سمت استفاده از این دانش برای مقابله گام برداشتند. نمونه این عملیات‌ها سرقت ایمیل‌های طبقه‌بندی شده کاخ سفید، وزارت خارجه و ستاد مشترک ارتش آمریکا توسط روسیه بود. آمریکا در چند سال گذشته، هزینه سنگینی را صرف جبران و ترمیم خسارات عملیات سایبری سال‌های ۲۰۱۴ و ۲۰۱۵ روسیه کرد ولی با این حال این کشور همچنان هدف حملات سایبری است.

هشدار درباره حمله سایبری فاجعه‌بار

بر همین اساس نیز «کمیسیون سولاریوم فضای مجازی ایالات متحده» که یک نهاد دوحزبی است و براساس قانون دفاعی سال ۲۰۱۹ تشکیل شده است، از وضعیت سایبری آمریکا ابراز نگرانی کرده و براساس تجزیه و تحلیل کمیسیون فدرال، از روبه‌رو بودن آمریکا با یک «حمله سایبری فاجعه‌بار» خبر داده که می‌تواند خسارت طولانی‌مدت بیش از بسیاری از آتش‌سوزی‌های جدی، سیل و توفان‌هایی که این کشور مجبور به تحمل آن است، ایجاد کند. «کمیسیون سولاریوم فضای مجازی ایالات متحده» در گزارش خود ادعا کرد که این کشور با تهدیدهای متعدد از سوی مجرمان سایبری و کشورها روبه‌رو است: «سرقت IP که مانع رشد طولانی‌مدت می‌شود، حملات مهم زیرساختی، جرایم اینترنتی و باج‌افزار، جاسوسی برای مزیت‌های ژئوپلیتیک و حملاتی که برای تضعیف دموکراتیک انجام می‌شود. این کمیسیون گفته «اتصال دیجیتال که تقریبا برای هر آمریکایی رشد اقتصادی، تسلط تکنولوژیکی و بهبود کیفیت زندگی را به همراه داشته است، یک معضل استراتژیک نیز داشته است. هرچه ارتباطات دیجیتال و ارتباطات دیجیتالی مردم بیشتر شود، دشمنان فرصت بیشتری برای از بین بردن زندگی خصوصی، ایجاد اختلال در زیرساخت‌های مهم و آسیب رساندن به نهادهای اقتصادی و دموکراتیک ما دارند. ایالات متحده اکنون در یک فضای سایبری فعالیت می‌کند که به سطحی از امنیت داده‌ها، قابلیت انعطاف‌پذیری و قابل اعتماد بودن احتیاج دارد که نه دولت ایالات متحده و نه بخش خصوصی درحال حاضر قادر به تهیه آن نیستند. علاوه‌بر این، فقدان سرعت، تخصص فنی و تلاش جمعی، هم در دولت ایالات متحده و هم بین بخش‌های دولتی و خصوصی، درحال افزایش است.» برای مقابله با این چالش‌ها، کمیسیون از رویکرد «لایه بازدارنده سایبری» که به‌منظور «شکل دادن به رفتار، انکار مزایا و تحمیل هزینه‌ها» طراحی شده است، حمایت کرده است. مورد اول ایالات متحده آمریکا را ملزم به همکاری با متحدان خود برای ارتقای رفتار مسئولانه در فضای مجازی می‌کند، دوم کار با بخش خصوصی برای افزایش امنیت و سومین مورد برای حفظ ظرفیت مقابله به‌مثل با دشمنان در فضای مجازی. این گزارش ۶ ستون سیاست و ۷۵ توصیه را برای کمک به ایالات متحده در رسیدن به آنجا ذکر کرده است. این موارد شامل پیشنهادهایی برای اصلاحات دولت ازجمله: «ایجاد کمیته‌های انتخاب دائمی مجلس و انتخاب سنا در زمینه امنیت سایبری، مدیر سایبری ملی تایید شده سنا و اختیارات جدید آژانس امنیت سایبری و زیرساخت (CISA) است که کارهای آن را در دولت پیش‌زمینه نشان می‌دهد.» برپایه تهدیدهای سایبری نگران کننده، بودجه پیشنهادی دولت آمریکا برای امنیت سایبری در سال مالی ۲۰۲۱ رقمی معادل ۱۸/۷۱ میلیارد دلار است. هزینه‌های فناوری اطلاعات دولت فدرال نیز ۸۸/۷۸ میلیارد دلار و بودجه فناوری اطلاعات دولت فدرال برای وزارت دفاع ۳۶/۷۴ میلیارد دلار تعیین شده است.

هزینه ۱۰/۵ هزار میلیارد دلاری جرایم اینترنتی

در مقاله‌ای که استیو مورگان برای Cybersecurity ventures درباره هزینه جرایم اینترنتی نوشته، تاکید کرده است که تا سال ۲۰۲۵ سالانه ۱۰/۵ تریلیون دلار این جرایم برای جهان هزینه دارد. او نوشته اگر جرایم اینترنتی به‌عنوان یک کشور محاسبه شود، با توجه به اینکه پیش‌بینی می‌شود جرایم اینترنتی در سال ۲۰۲۱ در کل ۶ تریلیون دلار خسارت وارد کند، سومین اقتصاد بزرگ جهان پس از ایالات متحده و چین خواهد بود. امنیت سایبری پیش‌بینی می‌کند هزینه‌های جرایم رایانه‌ای جهانی طی ۵ سال آینده ۱۵ درصد رشد کند و سالانه تا سال ۲۰۲۵ به ۱/۰۵ تریلیون دلار برسد درحالی که این رقم در سال ۲۰۱۵ به ۳ تریلیون دلار رسیده است. این نشان‌دهنده بزرگ‌ترین انتقال ثروت اقتصادی در تاریخ است، انگیزه‌های نوآوری و سرمایه‌گذاری را به خطر می‌اندازد، از نظر خسارت وارده از بلایای طبیعی در یک سال بسیار بزرگ‌تر است و از تجارت جهانی همه داروهای عمده غیرقانونی سودآورتر خواهد بود. هزینه‌های جرایم اینترنتی شامل خسارت و تخریب داده‌ها، پول‌های سرقت‌شده، بهره‌وری از دست رفته، سرقت مالکیت معنوی، سرقت داده‌های شخصی و مالی، اختلاس، کلاهبرداری، اخلال در روند عادی تجارت، تحقیقات پزشکی قانونی، بازسازی و حذف و هک شدن داده‌ها و سیستم‌ها و آسیب به اعتبار است.

جدا از جرایم سایبری، در حوزه دولت‌ها نیز توجه ویژه‌ای به حملات سایبری می‌شود. در بین تمام جرایم از این دست، حملات دولتی با توجه به پشتیبانی مالی، به‌مراتب تبعات بیشتری برای کشور هدف دارد. تد کوپل در پرفروش‌ترین کتاب خود در سال ۲۰۱۶ نشان داده که حمله سایبری عمده به شبکه برق آمریکا احتمال دارد ویرانگر باشد و آمریکا نیز به طرز تکان‌دهنده‌ای برای آن آماده نیست.

تقابل با آمریکا در سایبر

اهمیت جنگ سایبری برای کشورهای دیگر در برابر آمریکا از این جهت افزایش یافته که این کشورها علاقه‌ای به تقابل نظامی با آمریکا ندارند اما از فرصت جنگ سایبری برای ضربه زدن به رقیب استفاده می‌کنند. یک کشور متخاصم، به جای بمب اتم یا موشک‌های قاره‌پیما، می‌تواند با فشار کلیدهای رایانه‌ای از هزاران کیلومتر دورتر، خسارات فاجعه‌بار وارد کند. حملات سایبری می‌تواند با هزینه بسیار کمتر، آسیب بسیار عمیق‌تری به زیرساخت‌های کشور هدف بزند. این موضوعی است که مقامات آمریکایی نیز بدان اعتراف کرده‌اند. به‌عنوان نمونه فرماندهی سایبری ارتش آمریکا اذعان کرده‌اند که شبکه‌های کامپیوتری آمریکا شامل ارتباطات پنتاگون در مقابل حملات سایبری آسیب‌پذیر هستند. استفن فوگارتی، فرمانده سایبری ارتش آمریکا در این باره گفته: «زیرساخت‌های منسوخ شبکه‌های کامپیوتری دستگاه‌های اجرایی کشور در تامین و ارائه گزینه‌های کنترل ناکام هستند. شبکه‌های ما در معرض حملات سایبری قرار دارند. برخی از دشمنان به صورت موفقیت‌آمیزی در این زمینه عمل کرده‌اند.»

سال گذشته «مایکا لودرمیلک» در گزارشی با عنوان «گسترش بحران ایران به فضای سایبری» به بررسی توان سایبری ایران به‌عنوان یکی از دشمنان آمریکا که از این قابلیت استفاده می‌کند، پرداخت و نوشت: «طی دو سال گذشته، شرکت‌های امنیتی و دولت آمریکا عملیات‌های سایبری ایران را که هدفش جاسوسی از نهادهای دولتی آمریکا، زیرساخت‌های حساس، سازمان‌های هوانوردی نظامی/تجاری، تولیدات کارخانه‌ها، شیوه مهندسی و دیگر بخش‌ها بوده، شناسایی کرده‌اند. هکرهای ایران همچنین بنا به گزارش‌های سامانه نام دامنه‌های اینترنت را هدف قرار داده‌اند و از سرویس‌دهندگان اینترنتی و شرکت‌های مخابراتی داده‌هایی را به‌دست آورده‌اند که می‌تواند حملات آینده را تسهیل کند.»

نویسنده مدعی است: «اگر ایران حملات سایبری مختل‌کننده‌اش را شدت دهد، می‌تواند شبکه برق آمریکا را (که پیش‌تر هم به آن نفوذ کرده بود)، شبکه‌های آب (که به آن هم رخنه کرده بود)، سامانه‌های مخابراتی (که از آنها داده‌هایی را استخراج کرده)، یا حتی مدیریت شهرها را هدف قرار دهد.»

بایدن «فشار حداکثری» را ادامه می‌دهد

مشاوران نامزد دموکرات انتخابات آمریکا درحال ترغیب وی هستند تا با حفظ مولفه‌های سیاست فشار حداکثری ترامپ علیه ایران، از آن به‌عنوان اهرم فشار برای متقاعدکردن تهران به تغییر برجام استفاده کند. به گزارش فارس، به‌رغم گفته جو بایدن درباره بازگرداندن آمریکا به توافق هسته‌ای ایران در دولت جدید آمریکا، نشریه صهیونیستی «اسرائیل هیوم» مدعی است به اطلاعات جدیدی دست یافته که نشان می‌دهد چند تن از مشاوران نامزد دموکرات که در آستانه ورود به کاخ سفید قرار دارد، تلاش می‌کنند وی را برای اتخاذ رویکردی درقبال ایران متقاعد کنند که برخی از مولفه‌های سیاست فشار حداکثری دولت ترامپ در آن حفظ شود. به نوشته این رسانه، بین برخی مشاوران بایدن این دیدگاه وجود دارد که اتخاذ لحن آشتی‌جویانه درمقابل ایران نتیجه معکوس خواهد داشت.

فلین: ترامپ رئیس‌جمهور می‌ماند

مشاور امنیت ملی سابق دولت آمریکا که به‌تازگی با فرمان عفو دونالد ترامپ از زندان آزاد شده، گفت ترامپ همچنان راه‌های زیادی برای باقی‌ماندن در قدرت پیش‌رو دارد و صددرصد رئیس‌جمهور بعدی آمریکاست. به گزارش فارس، مایکل فلین در مصاحبه با شبکه «فاکس‌نیوز» گفت: «در درجه اول، رئیس‌جمهور همچنان راه‌های زیادی دارد که در جریان است و اگر از من بپرسند که در مقیاس یک تا ۱۰ بگویم چه کسی رئیس‌جمهور بعدی خواهد شد، با شماره ۱۰ می گویم دونالد ترامپ.» فلین روز شنبه هم در جمع هواداران رئیس‌جمهور آمریکا به سخنرانی پرداخت. او در جمع معترضان به نتیجه انتخابات ریاست‌جمهوری آمریکا گفت: «اکنون زمان حساسی است. باید دعا کنیم تا حقیقت بر دروغ، عدالت بر نقض قانون و تقلب و صداقت بر فساد پیروز شود.»

تعطیلی بندر جده به‌دنبال حملات انتحاری

بامداد روز گذشته یک نفتکش بریتانیایی در بندر جده عربستان مشرف به دریای سرخ به وسیله قایق‌های انتحاری مورد حمله قرار گرفت. به گزارش مهر به نقل از بی‌بی‌سی، یک منبع مسئول در وزارت انرژی سعودی درباره این حمله مدعی شد: «این اقدام تروریستی اندکی پس از حمله به کشتی دیگری و علیه ایستگاه توزیع فرآورده‌های نفتی در شمال جده و نیز سکوی تخلیه فرآورده‌های نفتی در جازان رخ می‌دهد. این اقدامات خرابکارانه ضدتاسیسات حیاتی عربستان در راستای هدف قرار دادن سعودی و مراکز حیاتی آن و برهم زدن امنیت و ثبات امدادرسانی انرژی و اقتصاد جهانی است.» منبع مسئول سعودی ادعا کرد: «تاثیر این اقدامات بر دریانوردی و امنیت صادرات نفت و آزادی تجارت بین‌المللی ویران کننده است.»

تونس از ترکیه پهپاد جنگی می‌خرد

منابع آگاه از قرارداد تسلیحاتی وزارت دفاع تونس با یک شرکت سازنده پهپاد ترکیه به ارزش ۸۰ میلیون دلار خبر دادند. به گزارش فارس، رسانه‌های ترکیه از اقدام وزارت دفاع تونس در امضای یک توافقنامه با یک شرکت تولید پهپادهای نظامی ترکیه به ارزش ۸۰ میلیون دلار خبر دادند. روزنامه «خبرترک» در شماره دیروز خود (دوشنبه-۱۴ دسامبر) نوشت: «این توافق شامل تحویل سه پهپاد از نوع («ANKA-S»عنقاء یا ققنوس)، سه ایستگاه کنترل زمینی پهپادها و آموزش ۵۲ عضو نیروی هوایی ارتش تونس است.» بنابر این گزارش، پس از دوسال مذاکره میان دو طرف درباره پهپادهای ANKA-S، سرانجام اواخر هفته گذشته دراین‌باره توافق شد. پیش از تونس، ماه پیش، اوکراین اعلام کرد در سال ۲۰۲۱ از ترکیه ۵ پهپاد تیپ «بایراکتار» خریداری خواهد کرد.