خبرنامه مدیریتی سراج
مرکز نرم‌افزار و سرویس وخدمات سازمان فضای مجازی سراج
اخبار فناوری اطلاعات وارتباطات
هفته نامه | سال دوم | شماره هفتاد و هفتم | ۱ آبان ۱۳۹۵
۷۷

آیا آیفون مدیر کمپین انتخاباتی کلینتون به دست نفوذگران افتاده است؟

ممکن است نفوذگران توانسته باشند اطلاعات ذخیره‌شده در آیفون و آیپد جان پودستا را پس از دستیابی به حساب iCloud وی، و نیز صندوق پستی جی‌میل و حساب توییترش پاک کنند.
پودستا، که به عنوان مدیر کمپین انتخاباتی هیلاری کلینتون فعالیت می‌کند، در ۱۳ اکتبر با افشای اطلاعات رایانامه‌ی خصوصی‌اش در فضای برخط مواجه شد.
همان‌طور که شواهد نشان می‌دهند، کارمندان ویکی‌لیکس یک بار دیگر در حذف اطلاعات شخصی از اسناد منتشره ناموفق عمل کرده‌اند؛ این اتفاق در چند ماه گذشته چندین بار رخ داده و حتی انتقاد ادوارد اسنودن را به خاطر عدم پاک‌سازی موارد افشاءشده به دنبال داشته است.

نفوذگران کنترل حساب توییتر پودستا را در دست گرفته‌اند
به گفته‌ی نفوذگران، که جریان شیطنت‌های خود را در 4chan منتشر کرده‌اند، یکی از رایانامه‌ها حاوی گذرواژه‌ی جی‌میل پودستا بوده است: «Runner456».
نفوذگران مدعی شده‌اند که توانسته‌اند به‌طور موفقیت‌آمیزی به رایانامه‌ی پودستا دستیابی پیدا کنند، سپس درخواست بازنشانی گذرواژه را برای حساب توییتر وی اعلام نمایند، در نهایت توییت «من جناحم را تغییر داده‌ام؛ در انتخابات ۲۰۱۶ به ترامپ رأی دهید. سلام Pol» را که در حال حاضر حذف شده، ارسال نمایند.
واژه‌ی «Pol» در این توییت به گروه Pol 4chan اشاره دارد؛ جایی که بحث و جدل‌هایی که هم‌اکنون حذف شده‌اند در آنجا صورت می‌گرفت.
نفوذگران اطلاعات آیفون و آیپد پودستا را پاک کردند
یک بازنشانی گذرواژه، نقطه‌ی ورود به حساب کاربری iCloud پودستا بوده است؛ جایی‌که نفوذگران به کمک قابلیت Find My iPhone توانستند اطلاعات آیفون و آیپد پودستا را پاک کنند.
نفوذگران یک سری اسکرین‌شات را برای اثبات نقش خود منتشر کرده‌اند. کمپین کلینتون فقط تصاحب حساب کاربری توییتر را تأیید کرده است، و راجع به حذف داده‌های آیپد و آیفون اظهار نظری نداشته است.

جولیان آسانژ زنده است اما به اینترنت دسترسی ندارد!

نگران نباشید! جولیان آسانژ زنده است و نفس می‌کشد، اما ظاهراً اتصال اینترنتی او مرده است.
در ساعات آغازین امروز، ویکی‌لیکس در توییتی اعلام کرد که اتصال اینترنتی بنیان‌گذارش، جولیان آسانژ، توسط یک «حزب دولتی» ناشناس قطع شده است.
این سازمان ناسودبر فقط اعلام کرد که «طرح‌های احتمالاً مناسبی را شروع کرده است»؛ ویکی‌لیکس هیچ توضیح دیگری در این رابطه نداد.
این توییت، بعد از ارسال توییت‌های سه‌بخشی مرموز ویکی‌لیکس که هر یک حاوی ۶۴ نویسه کد هستند، ارسال گردید. این توییت‌ها باعث شدند شایعه‌ی «مرگ آسانژ» بر سر زبان‌ها بیافتد.
در واقع این توییت‌ها به اکوادور، وزیر امور خارجه‌ی آمریکا جان کری، اداره‌ی امور مشترک‌المنافع و خارجه‌ی انگلستان اشاره دارند.
علاوه بر این، یکی از کاربران Reddit بیان داشت که این توییت‌ها شامل «هش‌هایی» است که به منظور حصول اطمینان از این موضوع به کار می‌روند که اطلاعاتی که در آینده توسط ویکی‌لیکس افشاء خواهند شد معتبر می‌باشند. ویکی‌لیکس این هش‌ها و عبارات درهم‌سازی شده را توییت کرده است. این متن‌ها گذرواژه‌هایی برای از گشودن قفل پرونده‌ها نیستند، بلکه یک اثر انگشت دیجیتالی به منظور تأیید صحت اخبار منتشره می‌باشند.
هچنین، هدف این کدهای ۶۴ نویسه‌ای به احتمال زیاد نوعی «پیش-تعهد» است، در واقع پیش-تعهد عملی در رمزنگاری و برای ارائه‌ی مدرکی مبنی بر آن است که هرگونه سند منتشرنشده‌ای با این رمزنگاری دست‌کاری نخواهد شد.

هدف بعدی ویکی‌لیکس کیست؟ جان کری؟
در نخستین توییت پیش-تعهد ویکی‌لیکس از جان کری یاد شده است، همان‌طور که می‌دانید جان کری سیاست‌مدار حزب دموکرات است که در حال حاضر پست وزارت امور خارجه‌ی آمریکا را بر عهده دارد.

افشای اطلاعات کمک‌کنندگان مالی به حزب جمهوری‌خواه

بار دیگر انتخابات ریاست جمهوری آمریکا در سر خط خبرها قرار گرفته و این بار صحبت از یک نفوذ است: نفوذی به نام NRSC. کمک‌های مالی اهداشده به کمیته ملی سناتوری جمهوری‌خواهان (NRSC)، در بازه ۱۶ مارس و ۶ اکتبر ۲۰۱۶ بر روی یک بستر مشخص مورد نفوذ واقع شده است. مهاجمان از بدافزاری استفاده کرده‌اند که به‌طور خاص برای سرقت داده‌های کارت اعتباری و اطلاعات شخصی طراحی شده است.

افرادی که پس از تاریخ ۶ اکتبر ۲۰۱۶ کمک‌های مالی خود را به این کمیته اهدا کرده‌اند، تحت تأثیر این نفوذ قرار نگرفته‌اند، چرا که NRSC به محض کشف این حمله سریعاً آن را برطرف کرده است.

این حمله مبتنی بر بدافزاری است که نخستین بار توسط متخصص امنیتی آلمانی، ویلیام دی‌گروت کشف شد. گروت که ترافیک این بستر را تحلیل کرده است، می‌گوید نفوذگران به داده‌های مربوط به ۳۵۰۰ تراکنش در ماه دست یافته‌اند.

«من نمی‌دانم مهاجمان چند کارت اعتباری را از فروشگاه جمهوری‌خواهان به سرقت برده‌اند اما می‌توانم دراین‌باره حدس‌هایی بزنم. به گفته TrafficEstimates، این فروشگاه هر ماه حدود ۳۵۰ هزار بازدید دارد. در یک تبدیل خوش‌بینانه با نرخ ۱ درصد، ۳۵۰۰ کارت اعتباری در هر ماه دزدیده شده که در نتیجه در این چند ماه مقدار ۲۱ هزار کارت اعتباری خواهد شد. مقدار ارزش هر کارت در بازار سیاه بین ۴ تا ۱۲۰ دلار است. اگر ارزش هر کارت سرقت‌شده را به‌طور میانگین ۳۰ دلار بگیریم، مهاجمان حدود ۶۰۰ هزار دلار به جیب زده‌اند.»

نفوذگران در جریان این نفوذ توانسته‌اند به داده‌هایی از جمله نام و نام‌خانوادگی اهداکننده مالی، آدرس رایانامه، جزئیات صورت‌حساب (آدرس، شهر، ایالت و کد پستی)، شغل، نوع کارت، شماره کارت، تاریخ انقضای کارت و کد امنیتی دست یابند. متخصصان امنیتی که بر روی داده‌های به سرقت‌رفته کار می‌کنند کشف کرده‌اند که این داده‌ها به 2 دامنه‌ی روسی ارسال شده‌اند. تحلیل‌های بیش‌تر نشان می‌دهد که نفوذگران ابتدا داده‌ها را به jquery-cloud.net ارسال می‌کردند اما بعداً به jquery-code.su تغییر مسیر داده‌اند. دامنه دوم هنوز فعال بوده و در اختیار Dataflowاست.

نفوذ به یک آژانس استرالیایی توسط نفوذگران خارجی

گزارش‌ها حاکی از آن است که جاسوسان خارجی یک نرم‌افزار مخرب را بر روی رایانه یکی از آژانس‌های دولتی استرالیایی نصب کرده و موفق شده‌اند تعداد زیادی اسناد دولتی را به سرقت ببرند. این رخنه امنیتی بر روی سامانه سازمان هواشناسی استرالیا که با سازمان دفاع نیز در ارتباط است رخ داده است. حمله مذکور در سال ۲۰۱۵ تشخیص داده شده و برخی منابع آن را به چین نسبت می‌دهند.

چین پیش از این هم به نفوذ به وبگاه‌های دولتی امریکا و شرکت‌های خصوصی متهم شده بود. در سال ۲۰۱۳، نفوذگران چینی متهم شدند که نقشه واحد مرکزی سازمان امنیت استرالیا را به سرقت برده‌اند.

مرکز امنیت سایبری استرالیا روز چهارشنبه این خبر را اعلام کرد اما اسمی از متهم اصلی نبرد. «ما هنوز نمی‌توانیم نامی از کشور خاصی در اتهام به این نفوذ ببریم، اما آنچه می‌توان گفت این است که این گروه جاسوسی سایبری زنده است و به فعالیت خود ادامه می‌دهد.»

در گزارش منتشر شده از سوی آژانس ملی امنیت سایبری استرالیا آمده است: «ما توانسته‌ایم حضور یک بدافزار RAT را، که در گروه نفوذگران پشتیبانی‌شده توسط دولت محبوبیت دارد، کشف کنیم. چند نمونه بدافزار دیگر نیز که با جرائم سایبری در ارتباط بوده‌اند کشف شده‌اند. این بدافزار RAT هم‌چنین برای بهره‌برداری از سایر شبکه‌های دولتی استرالیایی استفاده شده است. شواهدی نیز موجود است که مهاجم مذکور به جستجو و نسخه‌برداری از تعداد نامشخصی اسناد دولتی پرداخته است.»

در این گزارش هم‌چنین آمده است: «درحالی‌که در چند سال اخیر تهدیدهای سایبری علیه بخش‌های مختلف دولتی، زیرساخت و صنایع رو به افزایش بوده‌اند، خطر گروه‌های تروریستی هنوز کم است. توانایی گروه‌های تروریستی جدای از بهره‌برداری از شبکه‌های اجتماعی و اینترنت برای مقاصد تبلیغاتی، هنوز بیشتر در سطح ابتدایی بوده و به نظر نمی‌رسد در آینده نزدیک پیشرفت چشم‌گیری داشته باشد.»

ایالات‌متحده آمریکا به دنبال اقدام تلافی‌جویانه سایبری علیه روسیه

چند روز قبل ایالات‌متحده آمریکا روسیه را متهم کرد که سعی کرده است در انتخابات ریاست جمهوری این کشور تداخل ایجاد کند. واشنگتن به‌طور رسمی روسیه را به سعی در این اختلال متهم کرده و گفته است اقدامات لازم را برای مقابله با این تهدید انجام می‌دهد.

دفتر مدیریت اطلاعات ملی به همراه وزارت امنیت داخلی بیانیه‌ای را به‌طور مشترک صادر کرده‌اند که در آن دولت روسیه به انجام یک سری اقدامات خرابکارانه در شبکه‌های سازمان‌های آمریکایی و حوزه‌های انتخاباتی ایالتی متهم شده است. در این بیانیه آمده است: «سازمان اطلاعات آمریکا به این اطمینان رسیده است که دولت روسیه به‌طور مستقیم در سوءاستفاده از رایانامه‌های افراد و مؤسسات آمریکایی از جمله سازمان‌های سیاسی نقش داشته است. انتشار رایانامه‌های مورد نفوذ واقع‌شده در وبگاه‌هایی مانند DVLeaks.com و WikiLeaks نشانه‌هایی را از هم‌جهت بودن این اقدامات با تلاش‌های روسیه آشکار می‌سازد. این سرقت‌ها و انتشار این اطلاعات در جهت اختلال در روند انتخابات آمریکا بوده است. ما همه تلاش خود را در جهت محافظت از مرزهای خود به‌خصوص فضای سایبری خواهیم کرد. این بدان معنا نیست که اذهان عمومی در جریان همه اقدامات انجام شده و یا اقدامات در دست انجام در آینده، قرار خواهد گرفت.»

روز جمعه معاون رئیس‌جمهور، جو بایدن در مصاحبه با شبکه خبری NBC گفته است ایالات‌متحده درباره این نفوذها با ولادمیر پوتین، رئیس‌جمهور روسیه صحبت خواهد کرد. «ما پیامی را به پوتین خواهیم رساند، اما ارسال این پیام در زمان مقتضی و بر اساس شرایطی خواهد بود که بیشترین تأثیر را داشته باشد.»

به گفته NBC سازمان سیا در حال آماده‌سازی برای حمله سایبری تلافی‌جویانه است که برای کنترل حملات سایبری کرملین طراحی می‌شود.

جو بایدن در ادامه می‌افزاید: «دولت اوباما در حال بررسی عملیات سایبری نهان علیه روسیه است تا مانع از اختلالات بیشتر در بستر انتخابات رسایت جمهوری شود.»

یوکیا آمانو می‌گوید: حمله‌ی سایبری علیه نیروگاه هسته‌ای چندین سال قبل اتفاق افتاده است

با توجه به گزارش رویترز، مدیر آژانس بین‌المللی انرژی اتمی، یوکیا آمانو گفت احتمال یک حمله سایبری موفقیت‌آمیز دو تا سه سال پیش در یک نیروگاه هسته‌ای که نامش ذکر نشده وجود دارد.

مدیر آژانس سازمان ملل متحد گفت این حمله‌ی سایبر باعث برخی مشکلات در این نیروگاه هسته‌ای شده است. همچنین این حمله منجر به اجرای یک سری اقدامات احتیاطی و امنیتی شده است. در این گزارش آمده است، او همچنین از حمله‌ی نظامی علیه نیروگاه‌های هسته‌ای هشدار داد.

آمانو گفت یک تلاش چهارساله برای قاچاق مقدار کمی اورانیوم غنی‌سازی‌شده وجود دارد که می‌تواند برای ساخت بمب کثیف مورد استفاده قرار گیرد. او در طول سفر به آلمان گفت این تهدید، یک تهدید واهی و خیالی نیست.

نگرانی زیادی از ماه آوریل وجود دارد که 44 درصد از مدیران بخش انرژی، آب و برق و گاز و نفت افزایش 50 تا 100 درصدی را در حملات موفقیت‌آمیز سایبری علیه این بخش‌ها گزارش داده‌اند.

نفوذگران وابسته به دولت، تأسیسات هسته‌ای ژاپن را هدف قرار دادند

یک مرکز تحقیقات هسته‌ای ژاپن مورد نفوذ واقع شد و در نتیجه‌ی آن 59 هزار پرونده به سرقت رفت. دانشگاه مرکزی تحقیقات ایزوتوپ هیدروژن تویاما، یکی از سازمان‌های مهم دنیا در تحقیقات تریتیوم است. تریتیوم، که با عنوان هیدروژن 3 نیز شناخته می‌شود، یک ایزوتوپ رادیواکتیو هیدروژن است که یک سوخت مهم برای همجوشی کنترل‌شده‌ی هسته‌ای و یک جزء کلیدی در بمب‌های هیدروژنی است. همچنین این ماده یکی از آلاینده‌ها در ساختمان آب در نیروگاه هسته‌ای فوکوشیما شماره 1 است.

با توجه به گزارش رسانه‌های ژاپنی در این نفوذ تحقیقات تریتیوم آزمایشگاه به همراه اطلاعات شخصی 1493 محقق به سرقت رفته است. مهاجمان 3 دسته داده در بازه‌های زمانی مختلف را به سرقت برده‌اند: دسامبر 2015، مارس 2016 و ژوئن 2016.

بدافزارِ استفاده‌شده در این سرقتِ داده، از طریق حملات فیشینگ نیزه‌ای در نوامبر 2015 تحویل داده شده است، زمانی‌که یک نفوذگر به‌عنوان یک دانشجوی دانشگاه توکیو بر روی پروژه‌های تحقیقاتی کار می‌کرد.

بررسی‌کنندگان می‌گوید در تحلیل و بررسی نمونه‌ی بدافزاری مشاهده کردند که این بدافزار از قبل برنامه‌نویسی شده بود و بر روی رایانه قربانی به دنبال کلمه‌ی IAEA می‌گشت که مخفف آژانس بین‌المللی انرژی اتمی سازمان ملل متحد است.

ویشال گوپتا، مدیر عامل شرکت Seclore، در رایانامه‌ای گفت: «نقض رخداده در مرکز تحقیقات ایزوتوپ هیدروژن دانشگاه تویاما یک مثال رساله‌ای از نوع تهدیدات سایبری پیشِ روی دانشگاه‌ها است. محققان برای نهادهای دولتی اهداف بسیار سودمندی هستند چرا که سرمایه‌گذاری روی سرقت داده‌ها و بررسی آن‌ها نسبت به انجام پروژه و تحقیقات ارزان‌تر است. در نتیجه دانشگاه‌ها باید گام‌هایی را انجام دهند تا مطمئن شوند که کار آن‌ها تحت حفاظت کامل اجرا می‌شود مخصوصاً زمانی‌که آن‌ها تحقیقات هسته‌ای انجام می‌دهند (این تحقیقات در تمامی کشورها به‌جز چند کشور، ممنوع است). کنترل‌های امنیتی حاضر که در سطح داده به کار می‌روند، نیاز است تا به‌گونه‌ای عملیاتی شوند که اطمینان حاصل شود که محققان هسته‌ای را در دام بدافزارها گرفتار نمی‌کنند.»

سازمان FBI به سرقت بیت‌کوین معادل 1.3 میلیون دلار از حساب یک مرد ماساچوستی رسیدگی می‌کند

در طول 2 ماه گذشته، سومین بازار بیت‌کوین جهان، Bitfinex طی یک نفوذ بزرگ، بیت‌کوین به ارزش 7.2 میلیون دلار را از دست داده است. مدت کوتاهی پس از اینکه این شرکت با سرقت بیت‌کوین معادل 72 میلیون دلار مواجه شد، یک کاربر Bitfinex از کمبریج، ماساچوست که نام او ذکر نشده، به پلیس شکایت کرد که 1.3 میلیون دلار از بودجه‌ی حساب او به سرقت رفته است.

پس از این اتفاق، پلیس کمبریج پیگیری این ماجرا را به FBI واگذار کرد که در کنار مقامات اروپایی با بازارهای بیت‌کوین سر و کار دارد تا به شکایات کاربران در ادمه‌ی نفوذ به Bitfinex رسیدگی کند.

این فرد ادعا می‌کند که بیت‌کوین‌هایی معادل با 3.4 میلیون دلار در کیف پول بیت‌کوین خود که توسط Bitfinex میزبانی می‌شد، داشت. به دنبال نقض بزرگ بیت‌کوینی که در ماه آگوست به وقع پیوست، در حساب او 2.1 میلیون باقی مانده است.

Bitfinex در ادامه به این فرد اطلاع داد که بیت‌کوین به ارزش 1.3 میلیون دلار از حساب اولیه‌ی او به سرقت رفته است ولی بعد از اینکه شرکت توکن‌های IOU را صادر کرد که اقدامی ضروری برای عملیاتی نگه داشتن این بازار بیت‌کوینی است، سرقتی که از حساب این فرد صورت گرفته به 720 هزار دلار کاهش یافت.

توکن‌های IOU یا BFX، قالبی از غرامت هستند که برای کاهش زیان‌های قربانی با فاکتور قابل‌توجهی ارائه شده است.

اگرچه جزئیات کامل هنوز نامشخص است، کاربران Bitfinex زیان وارده بر بودجه‌هایشان در کنار توکن‌های IOU را تایید کردند که برای تمامی کاربران قربانی این نقض صادر شده است.

هنوز قابل استفاده بودن این توکن‌ها مشخص نیست. نه توضیحی در خصوص توکن‌های ارائه‌شده توسط Bitfinex هنوز مشخص است و نه هنوز مسائل حقوقی آن تعیین شده است.

برای گزارش وقوع رخداد به عنوان کاربر Bitfinex، می‌توانید به این پیوند مراجعه کنید. این لحظه جزئیات بیشتری از ماجرا هنوز مشخص نیست .

پس از وقوع این نقض بیت‌کوین معادل 72 میلیون دلار، بازار بیت‌کوین هنگ‌کنگ، جایزه‌ی 3.5 میلیون دلاری برای کسی که اطلاعاتی ارائه کند که موجب بازیابی بیت‌کوین‌های به سرقت‌رفته شود، تعیین کرده است.