خبرنامه مدیریتی سراج
مرکز نرم‌افزار و سرویس وخدمات سازمان فضای مجازی سراج
اخبار فناوری اطلاعات وارتباطات
۹۷
هفته نامه | سال دوم | شماره نود و هفتم | ۲۱ اسفند ۱۳۹۵

چگونه یک اشتباه تایپی، سرویس S3 آمازون و بخش وسیعی از اینترنت آمریکا را از کار انداخت؟

گزارش‌ها حاکی از آن است که اوایل این هفته بخش عمده‌ای از آمریکا با قطعی اینترنت مواجه شده است. این قطعی اینترنت به‌دنبال گسترش و توزیع یک بدافزار یا حمله‌ی سایبری نبوده است. بلکه این مشکل ناشی از یک اشتباه تایپی بوده است.

شرکت آمازون روز پنج‌شنبه اعتراف کرد یک اشتباه تایپی در وارد کردن دستوراتِ عیب‌یابی مربوط به سامانه‌های صدور صورت‌حساب، روز سه‌شنبه باعث قطعی برخی از سرویس‌های وب آمازون به مدت 5 ساعت شده است.

این موضوع باعث شده بود صدها سرویس و وب‌گاه از دسترس خارج شوند و در برخی دیگر از وب‌گاه‌ها نیز در بارگذاری تصاویر و پیوندها مشکلاتی وجود داشت. این اشکال باعث سردرگمی تعداد زیادی از کاربران اینترنت در سطح جهان شده بود. از جمله وب‌گاه‌هایی که تحت تأثیر این اشتباه قرار گرفته‌اند می‌توان Quora، Slack، Trello، Soundcloud، Splitwise و IFTTT را نام برد.

اصل ماجرا چه بوده است؟

صبح روز سه‌شنبه اعضای گروه سرویس ذخیره‌سازی ساده‌ی (S3) آمازون در حال عیب‌یابی سامانه‌ی صدور صورت‌حساب بودند. در قسمتی از این فرآیند، مسئولان مجبور شدند برخی از سرویس‌های این سامانه را از حالت برخط خارج کنند اما متأسفانه به اشتباه سرویس‌های بسیار زیادی را از کار انداختند.

آمازون گفت: «متأسفانه یکی از ورودی‌های دستور مورد نظر نادرست وارد شده و تعداد زیادی از سرویس‌ها از کار افتادند. کارگزارهایی که سهواً حذف شده‌اند توسط دو زیرسامانه‌ی S3 دیگر پشتیبانی می‌شوند.» مسئله‌ی دیگری که وجود دارد این است که چرا راه‌اندازی مجدد این سرویس‌ها اینقدر طولانی شده است؟ آمازون در پاسخ گفت این کارگزارها و سرویس‌ها سال‌ها بود که مجدداً راه‌اندازی نشده بود.

معاون دونالد ترامپ از یک حساب AOL استفاده می‌کرد که مورد نفوذ قرار گرفت

مایک پنس، معاون رئیس جمهور دونالد ترامپ، هیلاری کلینتون را برای استفاده از کارگزارهای رایانامه‌ی شخصی سرزنش می‌کرد و معتقد بود این کار باعث شده اطلاعات طبقه‌بندی شده‌ی او در معرض حملات نفوذگران قرار بگیرد.

اینک شواهد نشان می‌دهد زمانی که پنس فرماندار ایندیانا بود از یک حساب شخصی AOL استفاده می‌کرد و رایانامه‌های مربوط به بحث‌های تجاری دولت را با آن ارسال و دریافت می‌نمود. گزارش‌ها حاکی از آن است که حساب کاربری او در تابستان گذشته مورد نفوذ قرار گرفته یعنی درست چند ماه قبل از آنکه او هیلاری کلینتون را به‌خاطر استفاده از کارگزارهای شخصی سرزنش می‌کرد.

استفاده از حساب AOL توسط پنس در یک مقاله‌ی 2100 کلمه‌ای روز پنج‌شنبه توسط خبرگزاری IndyStar منتشر شده است. مقامات دولتی از اعلام تعداد رایانامه‌های تحت تأثیر قرار گرفته امتناع می‌کنند چرا که این اطلاعات را محرمانه و حساس دانسته و نمی‌خواهند این موضوع به‌طور عمومی مطرح شود.

در خبرها آمده است پنس از این حساب از اواسط دهه‌ی 1990 تا سال 2016 که این حساب مورد نفوذ قرار گرفته، استفاده کرده است. به‌عبارت دیگر پنس سه سال از دوره‌ی چهارساله‌ی فرمانداری خود از این حساب رایانامه استفاده کرده است. نفوذگری که به حساب کاربری AOL حمله کرده از آن برای ارسال هرزنامه به مخاطبان پنس استفاده کرده است. در این هرزنامه‌ها ادعا شده پنس و همسرش در فلیپین به کمک‌های مالی نیاز دارند. پنس در ادامه استفاده از این حساب را کنار گذاشت و حساب AOL دیگری را ایجاد کرد.

توانایی نفوذگران در دستیابی به فهرست مخاطبان پنس نشان می‌دهد، مهاجمان قادر هستند صندوق ورودی و خروجی رایانامه‌های او را نیز مشاهده کنند. نفوذ به حساب پنس به 2 سال بعد از اطلاع‌رسانی شرکت AOL برمی‌گردد. زمانی‌که این شرکت اعلام کرد تعدادی از حساب‌ها آلوده شده و کاربران باید گذرواژه‌های خود را تغییر دهند.

ویکی‌لیکس تمامی قابلیت‌های نفوذ سازمان سیا را افشاء کرد

ویکی‌لیکس به آنچه که هفته‌ی پیش وعده داده بود عمل کرد و تمام قابلیت‌های سازمان سیا با نام Vault 7 را منتشر ساخت. جولیان آسانژ ادعا می‌کند پرونده‌هایی که منتشر کرده مجموعه‌ای بسیار جامع از ابزارهای جاسوسی آمریکا است. در مجموع 8761 سند مربوط به قابلیت‌های نفوذ سازمان سیا منتشر شده است. ویکی‌لیکس اعلام کرده این سری اول افشای ابزارهای Vault 7 است.

در این پرونده‌ها چه چیزی وجود دارد؟ ویکی‌لیکس مدعی شده سازمان سیا دارای نرم‌افزاری است که به این سازمان امکان می‌دهد بر روی دستگاه‌های الکترونیکی مدرن از جمله آیفون، دستگاه‌های اندرویدی، رایانه‌ها و تلویزیون‌های هوشمند کنترل کامل داشته باشند.

ویکی‌لیکس اعلام کرده سازمان سیا اخیراً کنترل خود بر روی ابزارهای نفوذ خود از جمله بدافزارها، تروجان‌ها، بهره‌برداری‌های روز-صفرم، بدافزارهای کنترل از راه دور و اسناد مرتبط با آن را از دست داده است. به نظر می‌رسد کل این مجموعه بالغ بر چند صد میلیون خط کد، کل ظرفیت نفوذ سازمان سیا را نشان می‌دهد. احتمالاً این آرشیو بین نفوذگران و پیمانکاران دولت آمریکا ردوبدل می‌شده و در نهایت یکی از این افراد این ابزارها را به دست ویکی‌لیکس رسانده است.

این منبع نقض داده می‌خواهد یک بحث عمومی در مورد امنیت، ایجاد، تکثیر و نگهداری دموکراتیک سلاح‌های سایبری راه بیندازد. هرچند همگان از قدرت فوق‌العاده‌ی نفوذ سازمان سیا باخبر هستند ولی مشاهده‌ی اعداد و ارقام مربوط به ابزارهای نفوذ این سازمان بر روی کاغذ بسیار تکان‌دهنده است. در ادامه داستان‌های بیشتری راجع‌به Vault 7 خواهیم شنید.

سازمان سیا از اشتباهات آژانس امنیت ملی آمریکا نکاتی را یاد گرفته است

افشای قابلیت‌های نفوذ سازمان سیا «Vault 7» توسط ویکی‌لیکس تأیید می‌کند که آژانس امنیت ملی آمریکا (NSA) حامی گروه نفوذ Equation بوده است. اسناد افشاءشده نشان می‌دهد سازمان سیا از اشتباهاتی که آژانس امنیت ملی آمریکا داشته، نکاتی را یاد گرفته است.

پرونده‌هایی که از سازمان سیا بدست آمده، نشان از قدرت نفوذ بالای این سازمان دارد. در یکی از اسنادی که توسط ویکی‌لیکس منتشر شده، مقاله‌ای با عنوان «اشتباهات Equation چه بوده و چگونه ما می‌توانیم آن‌ها را تکرار نکنیم؟» مشاهده شده است.

عملیات گروه Equation و ارتباط آن با آژانس امنیت ملی آمریکا در سال 2015 میلادی توسط آزمایشگاه کسپرسکی توضیح داده شده بود. در این مقاله یک بحث عمومی در این خصوص برگزار شده است. شرکت‌کنندگان در این بحث معتقدند یکی از بزرگ‌ترین اشتباهات آژانس امنیت ملی آمریکا این بود که کدهای اشتراکی در ابزارهای این سازمان، دارای یک رمزنگاری ویژه بود و باعث شد محققان امنیتی از طریق آن بتوانند بدافزارهای مختلف را به گروه Equation نسبت دهند.

علاوه بر استفاده از الگوریتم رمزنگاری ویژه، سازمان سیا چند اشتباه دیگر را نیز برای آژانس امنیت ملی آمریکا متصور شده از جمله اینکه از بهره‌برداری‌ها استفاده‌ی مجدد کرده بود، نام ابزارهای داخلی را در کدهای خود استفاده می‌کرد و از mutex منحصربفرد بهره می‌برد.

یکی از کاربران شرکت‌کننده در بحث گفته است: «استفاده از کد مشترک بزرگ‌ترین عاملی بوده که به کسپرسکی اجازه داده تمامی این بدافزارها را به یک گروه نسبت دهد. خرید و استفاده از دامنه‌های دستور و کنترل، دومین اشتباه مسلم NSA بوده است چرا که در بررسی‌ها، بیشترین بخشی که مورد تحلیل و بررسی قرار می‌گیرد، این زیرساخت‌ها است.»

پرونده‌های Vault 7 نشان می‌دهد سازمان سیا، فقط از اشتباهات آژانس امنیت ملی نکاتی را یاد نگرفته است بلکه از بدافزارها و بهره‌برداری‌هایی که در دنیای واقعی مورد استفاده قرار می‌گرفت نیز بهره برده است. از جمله‌ی این بدافزارها می‌توان شیمون، UpClicker و کیت‌های بهره‌برداری از تأسیسات هسته‌ای را نام برد.