سراج

۲۱ اسفند ۱۳۹۵

شماره ۱۰۳

خبرنامه کارشناسی
اخبار فناوری اطلاعات و ارتباطات

مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج

هفته نامه | شماره صد و سوم | سال دوم | ۷۰ صفحه

Expert Bulletin News

Information Communication Technology

2th year 2017 | Weekly bulletin

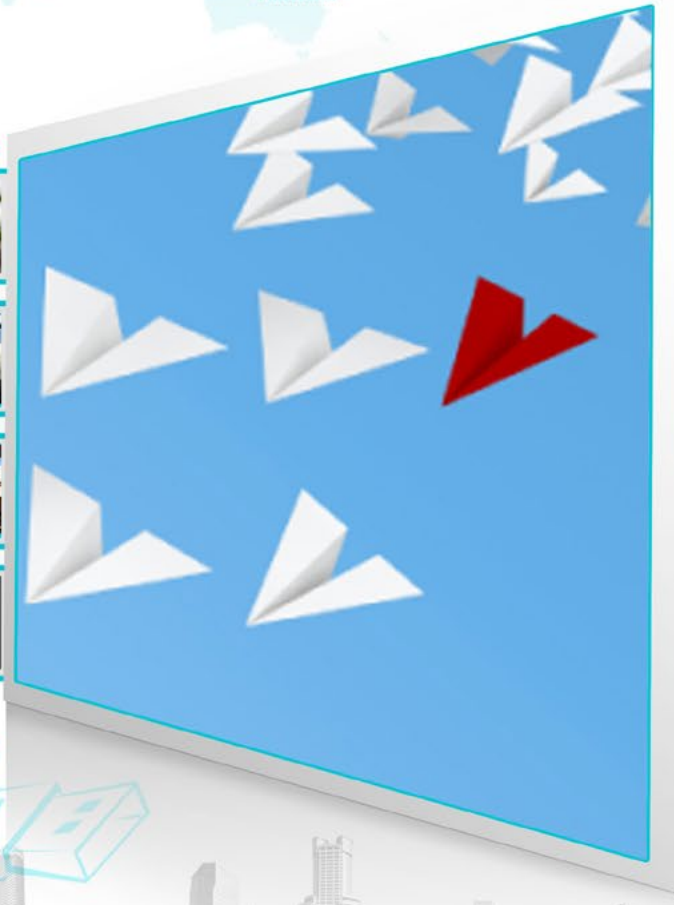
در این شماره می‌خوانید:

شرکت گوگل ۳۵ آسیب‌پذیری حیاتی را در اندروید وصله کرد

کریس ویکری اعلام کرد یک نقض داده‌ی عظیم را کشف کرده است

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

با انتشار نسخه‌ی جدید وردپرس، ۶ آسیب‌پذیری وصله شد

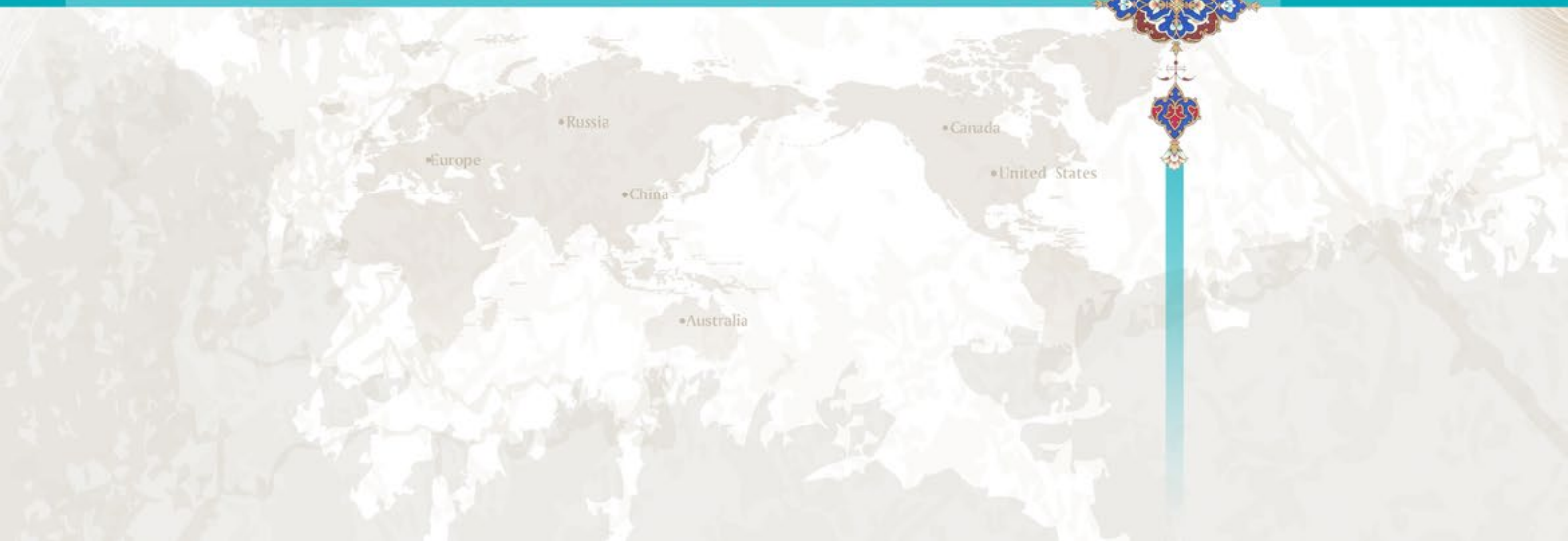


بسم الله الرحمن الرحیم

آگاهی و بصیرت

بنده بارها این جبهه های سیاسی و صحنه های سیاسی را مثال می زنم به جبههٔ جنگ. اگر شما در جبههٔ جنگ نظامی، هندسه زمین در اختیارتان نباشد، احتمال خطاهای بزرگ هست.

مقام معظم رهبری (مد ظله العالی)



فهرست مطالب

فصل اول: اخبار عمومی

شرکت گوگل 35 آسیب‌پذیری حیاتی را در اندروید وصله کرد. ۷
در ویندوز 10، کنترل بیشتری بر روی به‌روزرسانی و حریم ۹
خصوصی خواهید داشت
هشدار به کاربران هنگام وارد کردن گذرواژه‌ها در صفحات ناامن ۱۱
در فایرفاکس ۵۲
شرکت گوگل ویژگی مرورِ امن را در سامانه‌های macOS گسترش می‌دهد. ۱۲
اپل تمامی بهره‌برداری‌های iOS سازمان سیا را وصله کرده است.. . . . . ۱۳
گوگل: ما بسیاری از آسیب‌پذیری‌های مورد استفاده توسط سازمان ۱۴
سیا را وصله کرده‌ایم
با به‌روزرسانی‌های متعدد، کاربران لینوکس در برابر ۱۵
نفوذهای سازمان سیا محافظت می‌شوند
برنامه‌ی جعلی Facebook Lite به تروجان آلوده شده و اطلاعات ۱۶
کاربران را به سرقت می‌برد
کلیدهای رمزگشایی باج‌افزار Dharma به‌طور برخط منتشر شد. ۱۷
اپل از کاربران می‌خواهد در iOS 10.3 احراز هویت دومرحله‌ای را فعال کنند. . ۱۸
تلگرام ملحق شدن شما به این پیام‌رسان را به کلاه‌برداران اطلاع می‌دهد. . . . ۱۹
چرا مهاجمان سایبری، تلفن‌های همراه را هدف قرار می‌دهند؟. ۲۰

فصل دوم: مدیریت امنیت

با بهره‌برداری از یک آسیب‌پذیری در اوبر، رایگان سفر کنید. ۲۳
شرکت Dahua یک دربِ پشتی در محصولات اینترنت اشیاء را وصله می‌کند. . . . ۲۴
بزرگ‌ترین سازنده‌ی کارت‌های اعتباری در آمریکا، در حال بررسی ۲۶
یک نقض داده است
از هر 5 وب‌گاه، یک مورد همچنان از 1-SHA استفاده می‌کند. ۲۷
کریس ویکری اعلام کرد یک نقض داده‌ی عظیم را کشف کرده است. ۲۸
از کار افتادن سرویس میزبانی Freedom و کاهش تعداد وب‌گاه‌ها ۲۹
در وب تاریک
ربات‌ها در برابر حملات سایبری آسیب‌پذیر هستند. ۳۰
از آسیب‌پذیری Cloudbleed بهره‌برداری صورت نگرفته است. ۳۱
بدافزار کشف‌نشده‌ی مک در وب تاریک به قیمت 40 . . . . . ۳۳
بیت‌کوین به‌فروش می‌رسد
در سرویس‌های مایکروسافت آسیب‌پذیری کشف کنید، ۳۵
دو برابر جایزه بگیرید!
شرکت ارسال‌کننده‌ی هرزنامه، 1.4 میلیارد رکورد متعلق ۳۶
به کاربران را لو داد

فهرست مطالب

فصل سوم: سیاست سایبری

چگونه یک اشتباه تایپی، سرویس S3 آمازون و بخش وسیعی از اینترنت آمریکا را از کار انداخت؟ ۳۸
معاون دونالد ترامپ از یک حساب AOL استفاده می‌کرد که مورد نفوذ قرار گرفت ۳۹
ارائه‌دهنده‌ی معروف سرویس رایانامه در شبکه‌ی گمنامی Tor، از دسترس خارج شده است ۴۰
ویکی‌لیکس تمامی قابلیت‌های نفوذ سازمان سیا را افشاء کرد. ۴۱
یک میلیون گذرواژه‌ی رمزگشایی‌شده‌ی یاهو و جی‌میل در وب تاریک به فروش می‌رسد ۴۲
سازمان سیا از اشتباهات آژانس امنیت ملی آمریکا نکاتی را یاد گرفته است. ۴۳
سناتورهای دموکرات پنسیلوانیا هدف حملات باج‌افزارها قرار گرفتند. ۴۴

فصل چهارم: اخبار فنی

بستر HackerOne به پروژه‌های متن‌باز سرویس رایگان ارائه می‌دهد. ۴۶
آسیب‌پذیری موجود در آپاچی Struts، در دنیای واقعی مورد بهره‌برداری قرار می‌گیرد ۴۷
کشف یک دربِ پشتی در تجهیزات اینترنت اشیاء متعلق به شرکت چینی DblTek ۴۸
با انتشار نسخه‌ی جدید وردپرس، 6 آسیب‌پذیری وصله شد. ۴۹
با استفاده از ابزارهای گوگل، سامانه‌ی ری‌کپچای این شرکت دور زده شد. ۵۰
آسیب‌پذیری در Slack و سرقت حساب‌های کاربری توسط مهاجمان. ۵۲
شبیه‌ساز سرویس‌های آسیب‌پذیر برای متااسپلویت منتشر شد. ۵۳
برای آسیب‌پذیری GDI ویندوز، وصله‌ی موقتی منتشر شد. ۵۴

فصل پنجم: اخبار تحلیلی

آی‌بی‌ام: بهره‌برداری از آسیب‌پذیری Shellshock هنوز هم آسان و ارزان است ۵۶
چگونه داده‌های دیجیتال را در DNA ذخیره‌سازی کنیم؟ ۵۸
برنامه‌ی Q شرکت آی‌بی‌ام شامل رایانه‌ی کوانتومی 50 کیوبیت است. ۶۰
بدافزار پاورشِل، از پروتکل DNS به‌عنوان زیرساخت دستور و کنترل استفاده می‌کند ۶۲
آسیب‌پذیری در توییتر به مهاجمان اجازه می‌دهد به حساب‌های قفل‌شده دست یابند ۶۴
محققان می‌توانند با SGX اینتل بدافزارها را مخفی کرده و ۶۵

فهرست مطالب

کلیدهای خصوصی را بدست آورند
در بدافزار شیمون 2.0 ماژول باج‌افزاری کشف شد. ۶۷
حملات بر روی پروتکل DNS: چگونه به سمت وب‌گاه‌های ۶۸
جعلی هدایت می‌شویم؟
در توزیع باج‌افزار، حملات RDP نسبت به هرزنامه‌ها پیشی گرفته‌اند. ۷۰

فصل اول

اخبار عمومی

اخبار عمومی

شرکت گوگل ۳۵ آسیب‌پذیری حیاتی را در اندروید وصله کرد

گوگل این هفته به‌روزرسانی امنیتی را برای بستر اندروید منتشر کرد که در این به‌روزرسانی بیش از 100 آسیب‌پذیری وصله شده بود و 35 مورد از این آسیب‌پذیری‌ها حیاتی محسوب می‌شدند.

در یک بولتن امنیت، شاهد دو سطح وصله‌ی امنیتی بودیم. در سطح وصله‌ی امنیتی 2017-03-01 تعداد 36 آسیب‌پذیری (11 حیاتی، 15 بالا، 9 متوسط و 1 پایین) وصله شده بود. در سطح وصله‌ی امنیتی 2017-03-05 نیز 71 آسیب‌پذیری (24 حیاتی، 32 بالا، 14 متوسط و 1 پایین) برطرف شده است.

آسیب‌پذیری‌هایی که در به‌روزرسانی 2017-03-01 وصله شده عبارتند از:

آسیب‌پذیری‌های حیاتی:

- 9 آسیب‌پذیری اجرای کد از راه دور در کارگزار رسانه
- یک آسیب‌پذیری RCE در OpenSSL و BoringSSL
- یک آسیب‌پذیری ارتقاء امتیاز در اعتبارسنج بازیابی

آسیب‌پذیری‌های سطح بالا:

- 3 آسیب‌پذیری اجرای کد از راه دور در پیام‌رسان AOSP، libgdx و کتابخانه‌ی Framesequence
- یک آسیب‌پذیری ارتقاء امتیاز در Audioserver
- یک آسیب‌پذیری ارتقاء امتیاز در NFC
- 9 آسیب‌پذیری منع سرویس در کارگزار رسانه

آسیب‌پذیری‌های سطح متوسط:

- یک آسیب‌پذیری ارتقاء امتیاز در مدیر مکان، وای‌فای، مدیر بسته‌ها و واسط کاربری سامانه
- آسیب‌پذیری افشای اطلاعات در پیام‌رسان AOSP و کارگزار رسانه
- یک آسیب‌پذیری منع سرویس در Setup Wizard و کارگزار رسانه

آسیب‌پذیری سطح پایین:

- یک آسیب‌پذیری منع سرویس در Audioserver

آسیب‌پذیری‌هایی که در وصله‌ی سطح 2017-03-05 برطرف شده عبارتند از:

آسیب‌پذیری‌های حیاتی:

- 19 آسیب‌پذیری ارتقاء امتیاز در مؤلفه‌های MediaTek، راه‌انداز GPU انویدیا، زیرسامانه‌ی شبکه‌ی کرنل و ...
- 5 آسیب‌پذیری مختلف در مؤلفه‌های کوالکام

آسیب‌پذیری‌های سطح بالا:

- 25 آسیب‌پذیری ارتقاء امتیاز در مؤلفه‌های مختلف

کوالـکام

• 6 آسـیب‌پذیری افشـای اطلاعـات در زیرسـامانه‌ی شـبکه‌ی کرنـل، راه‌انـداز MediaTek، راه‌انـداز GPU انویدیـا و مؤلفه‌هـای کوالـکام

• یـک آسـیب‌پذیری منـع سرویـس در زیرسـامانه‌ی رمزنـگاری کرنـل

آسیب‌پذیری‌های سطح متوسط:

• یک آسیب‌پذیری ارتقاء امتیاز در راه‌انداز دوربین کوالکام

• 13 آسـیب‌پذیری افشـای اطلاعـات در مؤلفه‌هـای مختلـف کوالـکام

آسیب‌پذیری سطح پایین:

• یـک آسـیب‌پذیری افشـای اطلاعـات در راه‌انـداز دوربیـن کوالـکام

گـوگل در مشـاوره‌نامه‌ی خـود اعـلام کـرد تمامـی ایـن آسـیب‌پذیری‌ها در وصلـه‌ی سـطح 2017-03-05 یـا قبل‌تـر وصلـه شـده اسـت. ایـن شرکـت در تـلاش اسـت ایـن آسـیب‌پذیری‌ها را توسـط سـازوکار به‌روزرسـانی over-the-air- بـر روی دسـتگاه‌های اندرویـدی اعـمال کنـد.

ASADAL INTERNET, INC. started its business in Seoul Korea in February 1998 with the fundamentalgoal of providing better internet services to the world. ASADAL stands for the "morning land" in ancient Korean. Asadal has about 25 staffs including well experienced web designers, programmers, and server engineers.

اخبار عمومی

در ویندوز ۱۰، کنترل بیشتری بر روی به‌روزرسانی و حریم خصوصی خواهید داشت

مایکروسافت می‌گوید، در به‌روزرسانی ویندوز 10 که قرار است ماه آینده منتشر شود، انتظار می‌رود کاربران بتوانند کنترل بیشتری بر روی به‌روزرسانی نرم‌افزارها و تنظیمات حریم خصوصی داشته باشند.

با اعمال این تغییرات، به‌روزرسانی‌ها، دیرتر از موعد نصب نشده و تغییرات ناشی از این به‌روزرسانی‌ها تأثیر زیادی بر روی سایر عملکردهای سامانه نخواهد داشت. علاوه بر آن، کاربران می‌توانند از مزایای حریم خصوصی و تنظیمات در مورد بخش جمع‌آوری داده‌ها بهره‌مند شوند. کاربران می‌توانند از طریق داشبورد مبتنی بر وب، این ویژگی‌های حریم خصوصی را کنترل کنند.

در یک پست وبلاگی، مدیر برنامه‌ی گروه سرویس و تحویل مایکروسافت می‌گوید، بهبودهای حاصل در ویندوز 10 را مدیون بازخوردهایی می‌دانیم که از کاربران از طریق کانال‌های ارتباطی، شبکه‌های اجتماعی و انجمن‌ها دریافت کردیم.

یکی از مهم‌ترین تغییراتی که در ویندوز 10 به‌وجود آمده نحوه‌ی نصب به‌روزرسانی‌ها است چیزی که کاربران نمی‌توانند کنترل خاصی بر روی آن داشته باشند. تاکنون این گزینه در ویندوز 10 وجود نداشت که کاربران باتوجه به نیازمندی‌های خود به‌روزرسانی‌ها را مطابق با میل خود نصب کنند. در نسخه‌های قبلی شاهد بودیم که پس از به‌روزرسانی، ممکن بود سامانه مجدداً راه‌اندازی شود که این در برخی مواقع باعث خراب‌کاری و بهم‌خوردن برنامه‌ی کاربر می‌شد.

در به‌روزرسانی ویندوز 10، تغییراتی در زمان‌بندی نصب به‌روزرسانی‌ها نیز ایجاد شده است. بنابراین در نسخه‌ی جدید کاربران می‌توانند دقیقاً مشخص کنند که یک به‌روزرسانی چه‌زمانی باید رخ بدهد، می‌توانند به‌روزرسانی یک برنامه را مجدداً زمان‌بندی کنند و یا یک به‌روزرسانی را به تعویق بیندازند. به گزارش کارشناسان مایکروسافت، کاربران می‌توانند به‌روزرسانیِ خاصی را تا مدت 3 روز به حالت تعویق در آورند.

زمان‌بندی «ساعت فعال» نیز به‌روزرسانی خواهد شد بنابراین زمانی‌که کاربر در حال استفاده از سامانه است و می‌خواهد به اجرای برنامه‌های خود ادامه دهد، فرآیند به‌روزرسانی به پایان نخواهد رسید. مثل سابق، همچنان کاربران می‌توانند گزینه‌ی راه‌اندازی مجدد را انتخاب کرده و به‌روزرسانی‌ها را نصب کنند.

مدیر برنامه‌ی مایکروسافت اشاره کرده است: «مثل همیشه، ما از ارزش به‌روز نگه داشتن سامانه‌ها مطلع هستیم و به شما توصیه می‌کنیم به‌طور پیش‌فرض نصب به‌روزرسانی‌ها را در ویندوز 10 انتخاب کنید تا هرلحظه از برنامه‌ها و ویژگی‌ها و به‌روزرسانی‌های امنیتی برخوردار شوید. با این حال اگر بخواهید کنترل بیشتری بر روی این به‌روزرسانی‌ها داشته باشید، می‌توانید از ویژگی‌های

جدید ویندوز 10 استفاده کنید.»

او در ادامه توضیح داد برای داشتن کنترل بیشتر بر روی فرآیند به‌روزرسانی، کاربران می‌توانند بر روی آیکونی که در صفحه‌ی تنظیمات به‌روزرسانی ویندوز وجود دارد، کلیک کنند. در این صفحه به کاربر اجازه داده می‌شود به‌روز بودن یا نبودن سامانه‌ی خود را اعتبارسنجی کند. او اعلام کرد ویژگی‌های جدید ویندوز برای کنترل به‌روزرسانی‌ها، برای بازه‌ی زمانی مشخصی، برای کاربران داخلی ویندوز فعال بوده و از آن‌ها بازخوردهایی دریافت خواهد شد.

سال گذشته مایکروسافت مجبور شد در خصوص جمع‌آوری داده از کاربران توضیح بدهد. فرانسه این غول فناوری را مجبور کرد تا جمع‌آوری داده از کاربران بدون رضایت آن‌ها را متوقف کند. انتظار می‌رود در نسخه‌ی جدید به‌روزرسانی ویندوز 10، بهبودهای محسوسی در امنیت این محصول حاصل شود. یکی از ویژگی‌ها این می‌تواند باشد، که کاربر نصب برنامه از منابعی غیر از فروشگاه رسمی مایکروسافت را مسدود کند. در به‌روزرسانی جدید می‌توان نصب برنامه‌های Win32 را مسدود کرده و از نصب ناخواسته‌ی بدافزارها جلوگیری کرد.

ASADAL INTERNET, INC. started its business in Seoul Korea in February 1998 with the fundamentalgoal of providing better internet services to the world. ASADAL stands for the "morning land" in ancient Korean. Asadal has about 25 staffs including well experienced web designers, programmers, and server engineers.

اخبار عمومی

هشدار به کاربران هنگام وارد کردن گذرواژه‌ها در صفحات ناامن در فایرفاکس ۵۲

در آخرین نسخه‌ی مرورگر فایرفاکس که این هفته منتشر شد، در صفحات ناامنی که کاربران گذرواژه‌های خود را در آن وارد می‌کنند، هشدار داده خواهد شد. شرکت موزیلا این تغییر را سال قبل معرفی کرده بود و می‌خواست از خطرات وارد کردن اطلاعات حساس در صفحات محافظت‌نشده کاربران را آگاه کند. هشداری که سال قبل منتشر شده بود مخصوص توسعه‌دهندگان بود و اینک آخرین نسخه‌ی این مرورگر تلاش دارد هشدارهایی را به کاربران بدهد.

با استفاده از فایرفاکس 52.0 کاربران هنگامی که در صفحات HTTP ناامن برای وارد کردن اطلاعات ورود خود قرار می‌گیرند، به آن‌ها هشدار داده می‌شود. در هر صفحه‌ای که از HTTPS پشتیبانی نمی‌کند، هنگام کلیک بر روی فیلدهای نام کاربری و گذرواژه، پیام «این ارتباط ناامن است» نمایش داده می‌شود.

از فایرفاکس 51 شرکت موزیلا آیکون خاکستری رنگی را در صفحاتی که از HTTPS پشتیبانی نمی‌کردند نمایش می‌داد تا کاربران از ایمن نبودن این صفحات مطلع شوند. در حال حاضر علاوه بر نمایش این آیکون، یک پیغام هشدار نیز برای کاربر نشان داده می‌شود. این پیام زمانی نمایش داده می‌شود که کاربر بر روی فیلدهای نام کاربری و گذرواژه کلیک می‌کند.

در فایرفاکس 52 ویژگی کوکی‌های محدودِ ایمن نیز پیاده‌سازی شده است. این ویژگی از اینکه صفحات ناامن HTTP کوکی‌هایی با ویژگی امن تنظیم کنند جلوگیری می‌کند. در یادداشتی که موزیلا اخیراً منتشر کرده اعلام شده است که این ویژگی از تنظیم کوکی‌هایی با ویژگی‌های مشابه با کوکی‌های امن جلوگیری می‌کند.

در این به‌روزرسانی فایرفاکس، همچنین چندین آسیب‌پذیری نیز برطرف شده است. آسیب‌پذیری‌های حیاتی عبارتند از: دور زدن سازوکارهای حفاظتی ASLR و DEP، خرابی حافظه هنگام مدیریت ErrorResult، آسیب‌پذیری استفاده پس از آزادسازی در زمان کار با رویدادها در اشیاء FontFace، آسیب‌پذیری استفاده پس از آزادسازی در زمان استفاده از addRange برای افزودن طیفی از اشیاء به اشیاء ریشه‌ی نادرست و برخی آسیب‌پذیری‌ها در بخش امنیت حافظه. آسیب‌پذیری‌های با درجه‌ی اهمیت بالا که در فایرفاکس 52 وصله شده عبارتند از: شکست در تقسیم‌بندی در Skia، سرقت تاریخچه و پیکسل با فیلترهای SVG، خرابی در حافظه‌ی جاوا اسکریپت در فرآیند پاکسازی افزایشی، استفاده پس از آزادسازی در ذخیره‌سازی بافر در libGLES.

فایرفاکس 52 از تمامی بسترهای موجود از جمله ویندوز، لینوکس و macOS پشتیبانی می‌کند. این نسخه همچنین بخشی از تمدید انتشار پشتیبانی (ESR) است و برای مدت یک سال از پشتیبانی برخوردار خواهد بود.

اخبار عمومی

شرکت گوگل ویژگی مرورِ امن را در سامانه‌های macOS گسترش می‌دهد

گوگل این هفته اعلام کرد می‌خواهد ویژگی مرور امن را در سامانه‌ی macOS گسترش دهد. این شرکت قصد دارد با این کار از کاربران کروم در برابر تزریق تبلیغات ناخواسته و تغییرات در تنظیمات مرورگرها محافظت کند.

کارشناسان گوگل در وبلاگ امنیتی این شرکت گفتند: «ویژگی مرور امن در دستگاه‌های macOS امنیت را گسترش می‌دهد و تجربه‌ی امنی را با جلوگیری از نمایش برنامه‌های ناخواسته و بدافزارها برای کاربران رقم می‌زند. بنابراین در ادامه کاربران macOS در بازدید از وب‌گاه‌های مخرب و بارگیری بدافزارها، هشدارهای بیشتری را مشاهده خواهند کرد.»

برنامه‌هایی که تبلیغات را نمایش می‌دهند، سیاستِ برنامه‌های ناخواسته‌ی گوگل را نقض کرده و زمانی که مرورگر کروم چنین فعالیتی را در وب‌گاه‌ها مشاهده کند، به کاربران مک هشدار داده می‌شود.

باتوجه به تنظیماتی که در مرورگر کروم وجود دارد، گوگل می‌خواهد مطمئن شود برنامه‌های مورد نظر نمی‌توانند تغییراتی را بدون مجوز در صفحات آغازین، صفحات خانگی و موتورهای جستجو ایجاد کنند.

گوگل اخیراً واسط برنامه‌نویسی را برای سامانه‌های مک با نام «لغو تنظیمات» راه‌اندازی کرده که به افزونه‌های کروم اجازه می‌دهد تا صفحات آغازین، صفحات خانگی و تنظیمات جستجو در مرورگرها را تغییر دهند. گوگل می‌خواهد این واسط برنامه‌نویسی، تنها راهِ تأییدشده برای اعمال تغییرات در تنظیمات کروم در سامانه‌های macOS و OS x باشد.

با این‌حال، فقط افزونه‌هایی می‌توانند از واسط برنامه‌نویسیِ لغو تنظیمات استفاده کنند که در فروشگاه رسمی گوگل تأیید شده باشند. از تاریخ 11 فروردین ماه، هر برنامه‌ای که بخواهد خارج از سیاست‌های گوگل، تغییراتی را در تنظیمات کروم اعمال کند، هشداری به کاربر نمایش داده خواهد شد.

اخبار عمومی

اپل تمامی بهره‌برداری‌های iOS سازمان سیا را وصله کرده است

همان‌طور که در خبرها شنیدیم، ویکی‌لیکس دوباره دست پر برگشته است. این وب‌گاه 8700 سند از قابلیت‌های نفوذ سازمان سیا را منتشر کرده است. این اسناد نشان می‌دهد سازمان سیا دارای بهره‌برداری‌های روز-صفرم است که با استفاده از آن‌ها می‌تواند به دستگاه‌های آیفون نفوذ کند. اما شرکت اپل ادعا می‌کند تمامی این بهره‌برداری‌ها در آخرین نسخه‌ی iOS وصله شده است. در اسنادی که ویکی‌لیکس منتشر کرده، جزئیاتی از آسیب‌پذیری‌ها گفته نشده و همچنین معلوم نیست سازمان سیا از آن‌ها استفاده کرده است یا خیر. با این شرایط، اپل چگونه فهمیده که این آسیب‌پذیری‌ها چیست و وصله شده است؟ با این‌حال روز سه‌شنبه این شرکت پس از افشای اسناد توسط ویکی‌لیکس، بیانیه‌ای را منتشر کرده است.

«شرکت اپل عمیقاً به حفظ حریم خصوصی و امنیت مشتریان متعهد است. فناوری‌هایی که امروزه در دستگاه‌های آیفون مورد استفاده قرار گرفته، نمونه‌ای از بهترین روش‌های امنیتی است و ما پیوسته در تلاش هستیم تا روش‌های خود را بهبود بدهیم. سخت‌افزار و نرم‌افزار محصولات ما به‌گونه‌ای طراحی شده تا در سریع‌ترین زمان، به‌روزرسانی‌ها را دریافت کنند. می‌توانیم بگوییم در حال حاضر 80 درصد از مشتریان ما از به‌روزترین سامانه عامل استفاده می‌کنند. هرچند بررسی‌های اولیه‌ی ما نشان می‌دهد که تمامی آسیب‌پذیری‌هایی که در اسناد سیا منتشر شده، در آخرین نسخه‌ی سامانه عامل iOS وصله شده ولی ما همچنان در تلاش هستیم به محض شناسایی آسیب‌پذیری جدید، آن را برطرف کنیم. ما همواره از مشتریان خود می‌خواهیم تا از آخرین نسخه‌ی سامانه عامل استفاده کنند تا مطمئن شوند که تمام به‌روزرسانی‌های امنیتی را دریافت کرده‌اند.»

شرکت اپل تنها شرکتی نیست که سازمان سیا قبلاً تلاش کرده تا به دستگاه‌های آن نفوذ کند. براساس اسنادی که ویکی‌لیکس منتشر کرده، در سال 2016 میلادی سازمان سیا 24 بهره‌برداری روز-صفرم برای اندروید داشت و یک حمله با نام «فرشته‌ی گریان» را علیه تلویزیون‌های هوشمند سامسونگ انجام داده بود. این حمله به این آژانس اطلاعاتی اجازه می‌داد از این تلویزیون‌های هوشمند به‌عنوان میکروفون برای ضبط مکالمات افراد استفاده کند. در ادامه این صداها برای کارگزار سازمان سیا ارسال می‌شد.

اخبار عمومی

گوگل: ما بسیاری از آسیب‌پذیری‌های مورد استفاده توسط سازمان سیا را وصله کرده‌ایم

شرکت گوگل مدعی شده بسیاری از آسیب‌پذیری‌هایی که در فهرست قابلیت‌های سازمان سیا وجود دارد را وصله کرده است. براساس اسنادی که ویکی‌لیکس منتشر کرده، سازمان سیا می‌تواند فناوری‌های معروف مانند اندروید شرکت گوگل و iOS اپل را هدف قرار دهد. نفوذگران سازمان سیا آسیب‌پذیری‌های روز-صفرم را کشف کرده و از آن بهره‌برداری می‌کردند. این نفوذگران تلاش داشتند تنظیمات رمزنگاری بر روی بسیاری از برنامه‌های پیام‌رسان را دور بزنند.

در بیانیه‌ی گوگل آمده است: «ما پس از مرور تمام اسناد افشاءشده به کاربران خود اطمینان می‌دهیم با به‌روزرسانی‌ها و سازوکارهای امنیتی که در کروم و اندروید وجود دارد، تعداد بسیار زیادی از این آسیب‌پذیری‌ها برطرف شده است. بررسی‌های ما ادامه دارد و در صورت لزوم، سازوکارهای حفاظتی و دفاعی بیشتری را پیاده‌سازی خواهیم کرد. امنیت همیشه برای ما در اولویت قرار داشته است.»

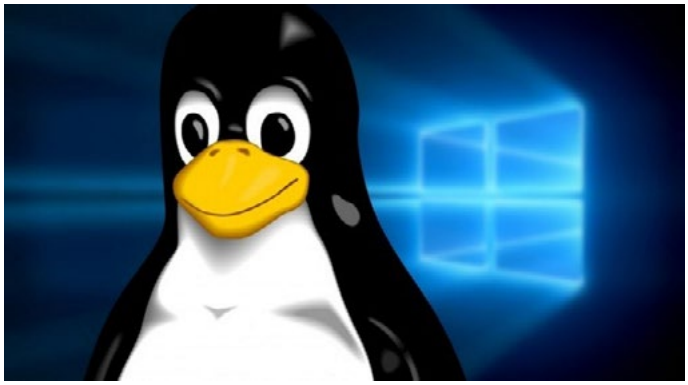
باتوجه به آنچه گوگل در بیانیه‌ی خود اعلام کرده، می‌توان متوجه شد که برخی از آسیب‌پذیری‌هایی که در فهرست سازمان سیا وجود دارد هنوز برطرف نشده و یا گوگل ایده‌ای در مورد اینکه این اشکالات چیست ندارد و این مسئله کاملاً طبیعی است. در حقیقت این اتفاق به این دلیل است که شرکت‌های بزرگی مانند گوگل می‌خواهند آژانس‌های اطلاعاتی پس از کشف آسیب‌پذیری روز-صفرم، آن‌ها را به این شرکت‌ها گزارش دهند. نگه داشتن این آسیب‌پذیری‌ها نزد خود و در ادامه بهره‌برداری برای اهداف این سازمان، میلیون‌ها نفر را در معرض خطر قرار می‌دهد.

شرکت‌های فناوری از رویکرد سازمان سیا در کشف و بهره‌برداری از آسیب‌پذیری‌های روز-صفرم اظهار نگرانی کرده‌اند. یکی از مدیران شرکت موزیلا می‌گوید: «به‌نظر می‌رسد سازمان سیا قصد دارد آسیب‌پذیری‌ها را انبار کند و در طرف دیگر ویکی‌لیکس نیز بجای اینکه پس از کشف این اسناد به شرکت‌های مربوطه گزارش دهد تا آسیب‌پذیری‌های مورد نظر را وصله کنند، دوست دارد صنایع دفاع سایبری را شوکه کند. ما امیدواریم همکاری بین نهادها افزایش یابد و شاهد چنین مسائلی نباشیم.»

اسناد و پرونده‌های Vault 7 که توسط ویکی‌لیکس منتشر شده نشان می‌دهد سازمان سیا روش‌های مختلفی برای نفوذ و کنترل گجت‌های مختلف دارد و همواره تلاش می‌کند از جدیدترین راه‌حل‌ها استفاده کند. بدافزارها و تروجان‌ها از نمونه‌هایی است که سازمان سیا به‌طور منظم بر روی آن‌ها کار می‌کند.

اخبار عمومی

با به‌روزرسانی‌های متعدد، کاربران لینوکس در برابر نفوذهای سازمان سیا محافظت می‌شوند



بنیاد لینوکس نیز به میدان آمده و در مورد اسناد Vault 7 که ویکی‌لیکس از قابلیت‌های نفوذ سازمان سیا منتشر کرده، صحبت کرده است. بنیاد لینوکس مدعی است به لطف متن‌باز بودن لینوکس، این سامانه عامل به‌طور مداوم با وصله‌های امنیتی به‌روزرسانی شده و به احتمال خیلی زیاد، تمامی آسیب‌پذیری‌های سازمان سیا را برطرف کرده است.

مدیرعامل بنیاد لینوکس می‌گوید: «لینوکس یک پروژه‌ی متن‌باز و بسیار فعال است. هزاران توسعه‌دهنده‌ی پیشرفته و داوطلب به‌طور مداوم برای بهبود آن کار کرده و آسیب‌پذیری‌های آن را برطرف می‌کنند. این موضوع به گروه هسته‌ی لینوکس امکان می‌دهد تا هرچند روز یک بار، به‌روزرسانی را منتشر کنند. این چرخه‌ی انتشار سریع به انجمن لینوکس اجازه می‌دهد تا هر آسیب‌پذیری را به سرعت وصله کرده و آن را برای کاربران منتشر کنند.»

تنها لینوکس نیست که اسناد افشاءشده را بررسی کرده و بیانیه صادر کرده است. در خبرهای قبل دیدیم که شرکت اپل اعلام کرده تمامی آسیب‌پذیری‌های مرتبط با iOS که سازمان سیا از آن‌ها استفاده می‌کند، در آخرین نسخه‌ی این سامانه عامل وصله شده است. گوگل نیز گفته است تقریباً بیشتر آسیب‌پذیری‌های روز-صفرم که در فهرست قابلیت‌های سازمان سیا وجود دارد را برطرف کرده است.

با انتشار اسناد Vault 7 ویکی‌لیکس دنیا را با قابلیت‌های نفوذ سازمان سیا شوکه کرد و نشان داد این قابلیت‌ها چقدر وسیع است. ولی این مسئله خیلی جای تعجب نداشت چرا که این کار سازمان اطلاعاتی مثل سیا است و این انتظار می‌رفت که این آژانس بدافزارهایی را توسعه داده و از آسیب‌پذیری‌های روز-صفرم برای اهداف خود بهره‌برداری کند.

نکته‌ی ناراحت‌کننده‌ای که در این اسناد وجود دارد این است که چرا سازمان سیا این آسیب‌پذیری‌های روز-صفرم را مخفی کرده و به شرکت‌های فناوری گزارش نداده تا میلیون‌ها نفر در معرض خطر قرار نگیرند. این سؤالی است که این روزها مدام پرسیده می‌شود. به هرحال اگر سازمان سیا توانسته این آسیب‌پذیری‌ها را کشف کند پس مسلماً افراد دیگری نیز موفق به کشف این آسیب‌پذیری‌ها شده‌اند و میلیون‌ها نفر در معرض خطر بودند.

اخبار عمومی

برنامه‌ی جعلی Facebook Lite به تروجان آلوده شده و اطلاعات کاربران را به سرقت می‌برد

یک نسخه از برنامه‌ی Facebook Lite در فروشگاه‌های ثالث فضای مجازی در حال توزیع است که به تروجان جاسوسی FakePlay آلوده شده است. این برنامه بجای اینکه توسط فیس‌بوک توسعه داده شده باشد، توسط چند فرد چینی توسعه داده شده است.

به گزارش محققان امنیتی این نسخه‌ی تقلبی از برنامه‌ی Facebook Lite خیلی جمع‌وجورتر از نسخه‌ی واقعی این برنامه است و داده‌های کمی را استفاده کرده و به بدافزار Android/Trojan.Spy.FakePlay آلوده شده است.

این برنامه تمامی قابلیت‌هایی که از او انتظار می‌رود را اجرا کرده و در پس‌زمینه نیز دست به فعالیت‌های مخرب می‌زند. این برنامه‌ی جعلی از گیرنده‌ها و سرویس‌های مخرب استفاده می‌کند تا خود را در قالب به‌روزرسانی گوگل منتقل کند.

محققان می‌گویند پس از راه‌اندازی دستگاه com.google.update.LaunchReceiver اجرا شده و بلافاصله پس از آن نیز گیرنده‌ی com.google.update.GetInst اجرا می‌شود. دومین برنامه‌ای که اجرا می‌شود حاوی کد مخربی است که برای سرقت اطلاعات شخصی و نصب برنامه‌های مخرب دیگر مورد استفاده قرار می‌گیرد. به‌عنوان مثال می‌تواند شناسه‌ی دستگاه، نسخه‌ی سامانه، آدرس مک، نام اپراتور شبکه، شماره سریال سیم‌کارت و اطلاعات دیگر را به سرقت ببرد.

از فروشگاه‌هایی غیر از فروشگاه رسمیِ گوگل برنامه بارگیری نکنید

محققان امنیتی می‌گویند: «معنای تحت‌اللفظی تروجان در ویکی‌پدیا این است که یک برنامه‌ی مخرب با هدف نفوذ بر روی رایانه‌ی شما نصب می‌شود. این بدافزار تلفن همراه نمونه‌ی واقعی یک تروجان است. این تروجان خود را در یک برنامه‌ی مشروع و قانونی تزریق کرده و اهداف مخرب خود را اجرا می‌کند و پشت پرده‌ی نام یک شرکت معتبر مخفی می‌شود.»

همان‌طور که گفتیم، باتوجه به نویسه‌هایی که در کد این تروجان کشف شده، برنامه‌ی جعلیِ Facebook Lite توسط چند نفر چینی توسعه یافته است. به‌دلیل اینکه کاربران چینی به فروشگاه رسمیِ گوگل دسترسی ندارند مجبور هستند برنامه‌های مورد نیاز خود را از فروشگاه‌های ثالث بارگیری کنند. بدون نظارت گوگل، تحت این شرایط مهاجمان می‌توانند کدهای مخرب خود را در داخل برنامه‌های قانونی توزیع کنند. پس توصیه می‌شود اگر به فروشگاه گوگل‌پلی دسترسی دارید، حتماً برنامه‌ها را از آن بارگیری و نصب کنید.

اخبار عمومی

کلیدهای رمزگشایی باج‌افزار Dharma به‌طور برخط منتشر شد

کلید رمزگشایی برای باج‌افزار Dharma به‌طور برخط منتشر شد. با استفاده از این ابزار، کاربرانی که به این بدافزار آلوده شده‌اند می‌توانند پرونده‌های رمزنگاری‌شده‌ی خود را بازیابی کنند.

روز گذشته فردی با نام کاربری gektar پستی در Pastebin منتشر کرده و پیوندی مربوط به انجمن پشتیبانی در BleepingComputer.com را معرفی کرد. او مدعی شده است در این انجمن، کلید رمزگشایی برای تمامی نسخه‌های باج‌افزار Dharma وجود دارد.

هنوز مشخص نیست این فرد کیست و چرا این کار را انجام داده و یا اینکه این کلیدهای رمزگشایی را از کجا آورده است اما مشخص است که این فرد به کد منبع باج‌افزار Dharma دسترسی دارد.

صرف‌نظر از اینکه این فرد کیست و چه هدفی دارد، نکته‌ی مهم این است که این کلیدها واقعی بوده و درست کار می‌کنند. محققان آزمایشگاه کسپرسکی و ESET این کلیدها را بررسی کرده به‌نظر می‌رسد که به‌درستی کار می‌کنند. این دو شرکت ابزار رمزگشایی Crysis خود را به‌روزرسانی کردند تا برای باج‌افزار Dharma نیز قابل استفاده باشد.

حتی اگر پرونده‌هایتان رمزنگاری شد، آن‌ها را نگه دارید!

باج‌افزار Dharma اولین بار در آبان ماه سال جاری مشاهده شد و یک نسخه‌ی جدید از باج‌افزار قدیمی با نام Crysis بود. پرونده‌هایی که تحت تأثیر این بدافزار قرار گرفته‌اند همگی دارای پسوندی مانند [email_address].dharma هستند و از این طریق می‌توان فهمید با چه باج‌افزاری طرف هستیم. در بخش آدرس رایانامه، آدرس مهاجمان برای برقراری تماس ذکر می‌شود.

جالب اینجاست که در آبان ماه برای باج‌افزار Crysis کلیدهای رمزنگاری به‌طور برخط افشاء شد و محققان می‌توانستند با استفاده از این کلیدها، ابزار رمزگشایی ساخته و به قربانیان این بدافزار کمک کنند.

درست است که برای مقابله با باج‌افزارها پیشگیری بهترین گزینه است ولی اگر روی قربانی باج‌افزار شدید و نخواستید باج درخواستی را پرداخت کنید، حتماً پرونده‌های رمزنگاری‌شده را نزد خود نگه دارید. ممکن است روزی کلیدهای رمزگشایی آن پیدا شده و شما رایگان بتوانید پرونده‌های خود را بازیابی کنید.

برخی مواقع، در دنیای باج‌افزارها، کلیدهای رمزگشایی بدون هیچ‌گونه توضیحی به‌طور برخط منتشر می‌شود. بعضی وقت‌ها نیز مقامات دولتی می‌توانند کارگزارهای دستور و کنترل متعلق به مهاجمان را ثبت و ضبط کرده و کلیدهای رمزگشایی را منتشر کنند. همچنین لازم است یادآور شویم که پویش NoMoreRansom.org با کمک شرکت‌های مختلف و مراجع قانونی راه‌اندازی شده تا به کاربران برای رمزگشایی پرونده‌ها کمک کنند.

اخبار عمومی

اپل از کاربران می‌خواهد در iOS 10.3 احراز هویت دومرحله‌ای را فعال کنند

به کاربرانی که از اپل iOS نسخه‌ی بتا 10.3 استفاده می‌کنند گزارشی مبنی بر فعال‌سازی احراز هویت دومرحله‌ای برای شناسه‌ی اپل از طرف این شرکت ارسال شده است که در دستگاه‌های اپل مانند آی‌پد، آیفون و سامانه‌های مک مورد استفاده قرار می‌گیرد تا داده‌های کاربر را بر روی iCloud همگام کرده و به اشتراک بگذارد. احراز هویت دومرحله‌ای شرکت اپل قرار است یک لایه‌ی امنیتی بیشتر برای داده‌های iCloud و دستگاه‌هایی که با شناسه‌های اپل ثبت شده‌اند، فراهم کند. به‌نظر می‌رسد با اقداماتی که در نسخه‌ی 10.3 صورت گرفته، اپل تلاش دارد کاربران را به استفاده از این ویژگی امنیتی تشویق کند.

احزار هویت دومرحله‌ای در دستگاه‌های شرکت اپل ویژگی جدیدی نیست و قبلاً نیز در سامانه عامل iOS9 و OS X وجود داشت. این ویژگی به‌تازگی برای داده‌های iCloud فعال شده است و این اقدام پس از نفوذهایی که به این سرویس انجام شد، صورت گرفته است.

تا قبل از انتشار نسخه‌ی 10.3 بتا iOS اپل هیچ‌وقت از طریق اعلان به کاربر اعلام نکرده بود که احراز هویت دومرحله‌ای را فعال کند ولی خبر خوبی که وجود دارد این است که اگر دستگاه شما دارای ملزومات سیستمی باشد، نیازی نیست برای فعال‌سازی این ویژگی‌ها منتظر یادآوری‌های اپل باشید.

اگر از iOS نسخه‌ی 9 یا بالاتر استفاده می‌کنید، می‌توانید این ویژگی را از طریق راهنمای زیر بر روی آیفون خود فعال کنید.

به بخش «تنظیمات» رفته و در انتهای این صفحه بر روی «iCloud» کلیک کنید. در قسمت بالای صفحه، شناسه‌ی اپل خود را وارد کنید. در صفحه‌ی بعدی، گزینه‌ی «امنیت و گذرواژه» را انتخاب کنید. در قسمت وسط صفحه گزینه‌ی «احراز هویت دومرحله‌ای» را مشاهده خواهید کرد. این گزینه را فعال کنید. ممکن است از شما برای اعتبارسنجی هویت، سؤالات امنیتی و یا جزئیات کارت‌های اعتباری شما پرسیده شود.

اخبار عمومی

تلگرام ملحق شدن شما به این پیام‌رسان را به کلاه‌برداران اطلاع می‌دهد

به‌نظر می‌رسد پیام‌رسان معروف تلگرام به‌خاطر یکی از ویژگی‌های خود دارای یک سری اشکالات حریم خصوصی است. محققان امنیتی می‌گویند تلگرام می‌تواند با نمایش دادن کاربران به نفوذگران، یک اشکال جدّی حریم خصوصی به دنبال داشته باشد.

یکی از دلایلی که بسیاری از افراد از تلگرام استفاده می‌کنند این است که گزینه‌ی رمزنگاری پیام‌ها برای کاربران اندروید و iOS را فراهم می‌کند. به‌طور همزمان، وقتی شما در تلگرام ثبت‌نام می‌کنید، این برنامه فهرست مخاطبان شما را پویش کرده و کسانی که این برنامه را نصب دارند، به شما نمایش می‌دهد. اینجاست که مشکل حریم خصوصی پیش می‌آید! اگر فردی شماره‌ی تلفن همراه شما را در فهرست مخاطبان خود داشته باشد، زمانی‌که شما وارد تلگرام می‌شود، در قالب اعلانی به او گفته می‌شود که شما به سرویس تلگرام ملحق شدید. محققان امنیتی در یک پست وبلاگی توضیح دادند: «اگر یک کلاه‌بردار در تلگرام ثبت‌نام کرده و شماره‌ی تماس شما نیز در فهرست مخاطبان او وجود داشته باشد، به او اعلام خواهد شد که شما تلگرام نصب کردید. بنابراین، تلگرام علاوه بر اینکه می‌تواند شما را با دوستانتان مرتبط کند، شما را مستقیماً به کلاه‌برداران وصل می‌کند. به‌همین ترتیب اگر شما شماره‌ی تماس کلاه‌بردار را داشته باشید، به‌محض ملحق شدن او به تلگرام، به شما اطلاع داده خواهد شد.»

این مشکل روز به‌روز بیشتر و بیشتر می‌شود چرا که کلاه‌برداران تلفنی به سرویس‌های این پیام‌رسان روی می‌آورند. مسئله وقتی بدتر می‌شود که هیچ راهی برای جلوگیری از اینکه دیگران بدانند شما از تلگرام استفاده می‌کنید، وجود ندارد.

مشکل زمانی بزرگ‌تر می‌شود که شما از این حساب‌ها با این ویژگی برای یک نهاد ثالث استفاده می‌کنید. به‌طور مثال، بسیاری از آژانس‌های اطلاعاتی این نوع از برنامه‌ها را به‌عنوان عامل خطر در نظر می‌گیرند. در حقیقت وقتی شما می‌خواهید از حریم خصوصی خود حفاظت کنید آن‌ها فکر می‌کنند شما اطلاعاتی برای مخفی کردن دارید.

باید به این نکته نیز اشاره کنیم که تنها پیام‌رسان تلگرام نیست که دارای این مشکل حریم خصوصی است چرا که سایر پیام‌رسان‌ها نیز از این ویژگی برای متصل کردن شما با دوستانتان استفاده می‌کنند. سایر پیام‌رسان‌ها مانند اسکایپ نیز این ویژگی را دارند. تفاوتی که بین تلگرام و سایر پیام‌رسان‌ها وجود دارد این است که شما انتظار دارید به‌دلیل رمزنگاری که تلگرام برای شما فراهم می‌آورد، از سطح بالایی از حریم خصوصی برخوردار شوید.

اخبار عمومی

چرا مهاجمان سایبری، تلفن‌های همراه را هدف قرار می‌دهند؟

شکی نیست که تلفن‌های همراه بخش اصلی زندگی روزمره‌ی افراد را تشکیل می‌دهند و کاربران می‌توانند تمامی وظایف روزمره‌ی خود را آسان‌تر و لذت‌بخش‌تر انجام دهند. در حالی‌که تلفن‌های همراه تلاش دارند زندگی را برای کاربران راحت‌تر کنند، از طرفی می‌توانند به هدفی برای مهاجمان سایبری نیز تبدیل شوند. در این پست می‌خواهیم بررسی کنیم چرا مهاجمان برای نفوذ به تلفن‌های همراه بسیار مشتاق هستند؟

تلفن همراهِ شما، همه‌چیز در مورد شما می‌داند

در سال‌های اخیر، میزان اطلاعاتی که در تلفن‌های همراه ذخیره شده، سر به فلک کشیده است. ارتباط بین برنامه‌ها باعث شده تا ما تمامی اطلاعات را درباره‌ی خود عرضه کنیم خواه این اطلاعات جزئیات حساب‌های بانکی باشد یا سلیقه‌ی ما در انتخاب پیتزا. برای مهاجمانی که می‌خواهند هویت کاربران را سرقت کنند، تلفن‌های همراه همچون معدنی از طلا هستند.

تلفن‌های همراه به وسیله‌ای در شرکت‌ها و سازمان‌ها تبدیل شده است

استفاده از فناوری «دستگاه خود را بیاورید» (DYOD) در حال تبدیل شدن به روشی است که بسیاری از سازمان‌ها در سراسر جهان از آن استفاده می‌کنند. نتایج پژوهش‌های محققان نشان می‌دهد در سال 2015 میلادی، 74 درصد از شرکت‌ها با فناوری‌های DYOD سازگار شده‌اند. برای مهاجمان سایبری، در این شرایط دستگاه‌های تلفن همراه به‌عنوان دروازه‌ای برای سرقت اطلاعات حساس سازمان‌ها محسوب می‌شود.

در امنیت ممکن است سهل‌انگاری رخ دهد

ظهور BYOD برای بسیاری از سازمان‌ها نیز دردسرساز شده است چرا که رویکرد یکپارچه‌ای برای حفظ امنیت این دستگاه‌ها اتخاذ نمی‌شود. در یک بررسیِ تحقیقاتی از مدیران و کارکنان سازمان‌ها، 45 درصد از پاسخ‌دهندگان اعلام کردند دستگاه‌های تلفن همراه بیشترین خطر را برای زیرساخت‌های شرکت به‌همراه دارند و ماهیت پراکنده‌ی تلفن‌های همراه دلیل اصلی این خطرات عنوان شده است.

گزینه‌ی تکمیل خودکار به بهترین دوست ما تبدیل شده است

یکی از دلایلی که باعث شده در تلفن‌های همراه ما اطلاعاتی بسیار بیشتر از گذشته وجود داشته باشد، این است که ما به‌دنبال راحتی هستیم. با استفاده از سرویس‌ها و برنامه‌های متعدد، شاهد هستیم که در صفحات ورود به سرویس‌ها، جزئیات و گواهی‌نامه‌های متعددی را مشاهده می‌کنیم. با این اوصاف ما رفته‌رفته تنبل‌تر می‌شویم. به‌عبارت دیگر ترجیح می‌دهیم تا از گزینه‌های تکمیل خودکار استفاده کرده و خود را در معرض خطرات مختلف قرار دهیم.

تلفن همراه شما، مسیری به سمت کیف پولتان است

ما می‌توانیم از تلفن همراه خود برای انتقال پول، پرداخت صورت‌حساب‌ها و به‌طور کلی به‌عنوان روشی برای پرداخت‌ها استفاده کنیم. کیف پول گوگل، سامانه‌های پرداخت اپل و سامسونگ را در بسیاری از تلفن‌های همراه مشاهده می‌کنیم و به‌گفته‌ی کارشناسان تعداد این برنامه‌ها در آینده بیشتر نیز خواهد شد. البته تنها اشکالی که این مسئله دارد این است که توجه مهاجمان سایبری به سمت تلفن همراه ما جلب می‌شود.

تلفن‌های همراه می‌دانند شما کجا هستید و کجا کار می کنید

در بسیاری از موارد ممکن است در پسِ پرده‌ی ردیابی شما، نیّت خوبی وجود داشته باشد و فناوری‌های مختلف بخواهند شما را از شرّ داده‌ها و اطلاعات اضافی خلاص کنند. به‌طور مثال فرض کنید از منزل خارج شده و می‌خواهید به رستوران بروید، یک برنامه با ردیابی شما می‌تواند نزدیک‌ترین رستوران را به شما معرفی کند. با این‌حال، نفوذ به سامانه‌ی GPS یک تلفن همراه کار خیلی سختی نیست.

بلوتوث

سال‌ها است که بلوتوث در تلفن‌های همراه مورد استفاده قرار می‌گیرد. اینک بلوتوث نیز مانند GPS به هدفی برای مهاجمان سایبری تبدیل شده است. تأثیر حملات بر روی بلوتوث می‌تواند باعث آلوده شدن اطلاعات کاربران شده و یا کم و بیش، کنترل دستگاه را در اختیار مهاجمان قرار دهد.

برخی از نفوذگران به‌طور ویژه بر روی تلفن همراه متمرکز شده‌اند

روش‌های مختلفی وجود دارد که مهاجمان از آن‌ها برای سرقت پول‌ها از طریق تلفن همراه استفاده می‌کنند. در کشورهایی مانند چین، به‌طور مثال، می‌توان با استفاده از بدافزار به دستگاه‌ها نفوذ کرده و با استفاده از شماره‌ی بیمه، مبلغ زیادی را به سرقت برد. این کلاه‌برداری‌ها نه تنها سودآور است بلکه می‌تواند به دستگاه‌های زیادی منتشر شود.

روش‌های بسیار عالی برای ارسال هرزنامه وجود دارد

همه از هرزنامه متنفرند. با این‌حال هرزنامه‌ها بخش جدایی‌ناپذیر بسیاری از حملات سایبری هستند. دلایل زیادی وجود دارد که مهاجمان می‌توانند تصمیم به ارسال هرزنامه بگیرند ولی بسیاری از مهاجمان، تلفن‌های همراه را بستر ایده‌آلی برای ارسال هرزنامه می‌دانند. این همان دلیلی عمده‌ای است که ارائه‌دهندگان سرویس به‌سختی می‌توانند نفوذگران را ردیابی و مسدود کنند.

کاربران در مورد خطرات، اطلاعات کافی ندارند

بسیاری از کاربران در بخش‌های فناوری، می‌دانند که بهترین واکنش در استفاده از لپ‌تاپ یا رایانه‌ی رومیزی چیست اما در تعیین اولویت‌ها و مشخص کردن بهترین راه‌حل‌ها، تلفن‌های همراه نادیده گرفته شده و در انتهای فهرست قرار دارند. شاید بسیار عجیب باشد ولی از سال 2005 میلادی، تلفن‌های همراه بیش از پیش هدف حملات سایبری قرار گرفته‌اند. با این‌حال وقتی ما بیشتر متوجه مسائل امنیتی می‌شویم، تهدیداتی که برای تلفن‌های همراه وجود دارد، بیشتر به چشم می‌خورد.

ASADAL INTERNET, INC. started its business in Seoul Korea in February 1998 with the fundamentalgoal of providing better internet services to the world. ASADAL stands for the "morning land" in ancient Korean. Asadal has about 25 staffs including well experienced web designers, programmers, and server engineers.

فصل دوم

مدیریت امنیت

مدیریت امنیت

با بهره‌برداری از یک آسیب‌پذیری در اوبر، رایگان سفر کنید

یک محقق امنیتی کشف کرد آسیب‌پذیری در برنامه‌ی اوبر وجود دارد که به کاربران اجازه می‌دهد به‌طور رایگان مسافرت‌های درون شهری خود را انجام دهند. آسیب‌پذیری که توسط این محقق هندی کشف شده به مهاجمان این امکان را می‌دهد با استفاده از حساب‌های اوبر به‌طور نامحدود و رایگان سوار وسایل نقلیه شوند. او مسافرت‌هایی را در آمریکا و هندوستان به‌طور رایگان انجام داد تا این آسیب‌پذیری را به گروه توسعه‌ی اوبر اثبات کند.

این آسیب‌پذیری مربوط به روش پرداخت در این برنامه است درست زمانی‌که کاربر می‌خواهد در وب‌گاه Uber.com برای خود حساب ایجاد کرده و اطلاعات پرداخت را وارد کند. در تنظیمات حساب کاربر می‌تواند انتخاب کند که کرایه‌ی سفر را نقدی به راننده بپردازند یا آن را به حساب اعتباری او منتقل کند.

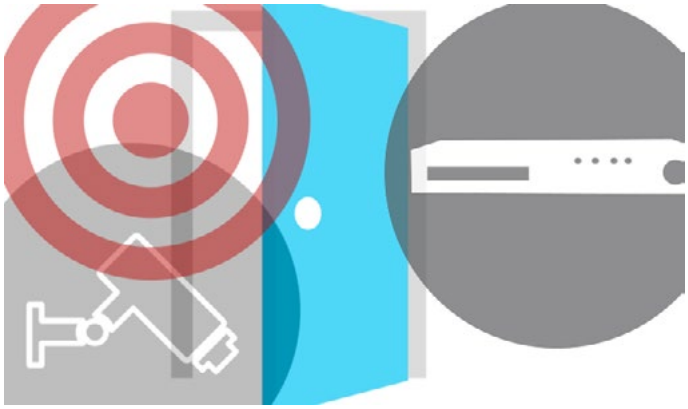
این محقق امنیتی کشف کرد اگر یک روش پرداخت نامعتبر انتخاب شود، مسافر می‌تواند به‌رایگان سفر خود را انجام دهد. به گزارش این محقق هندی، آسیب‌پذیری در داخل یک درخواست POST به dial.uber.com وجود دارد. برای تکرار بهره‌برداری از این آسیب‌پذیری، کاربر می‌تواند مقدار نامعتبری را در فیلد payment_method_id این درخواست POST وارد کند.

این محقق آسیب‌پذیری را به گروه اوبر در قالب برنامه‌ی پاداش در ازای اشکال بر روی بستر HackerOne گزارش کرده است. در این برنامه قرار است برای گزارش آسیب‌پذیری بر روی چندین رویس اوبر، مبلغی بین 100 تا 10 هزار دلار جایزه تعلق بگیرد. به‌نظر می‌رسد این آسیب‌پذیری در مرداد ماه کشف شده و همان روز نیز توسط گروه اوبر وصله شده است. او برای گزارش این آسیب‌پذیری 5 هزار دلار جایزه دریافت کرده است.

علاوه بر گزارش این آسیب‌پذیری، این محقق ویدئویی را برای نمایش نحوه‌ی بهره‌برداری از آن منتشر کرده است. این محقق از سال 2013 میلادی یکی از اعضای بستر HackerOne است و توانسته آسیب‌پذیری‌هایی را بر روی سرویس‌هایی مانند توییتر، یاهو و Slack کشف کند. رتبه‌ی این محقق در HackerOne برابر با 29 و در برنامه‌ی پاداش در ازای اشکال اوبر نیز 14 است. او در کشف آسیب‌پذیری‌های توییتر نیز در مقام سوم قرار دارد.

مدیریت امنیت

شرکت Dahua یک دربِ پشتی در محصولات اینترنت اشیاء را وصله می‌کند



یک شرکت در کالیفرنیا که محصولاتی مانند دوربین‌های CCTV، IP و DVR ها تولید می‌کند، در تلاش است یک دربِ پشتی در محصولات خود را وصله کند. شرکت Dahua برای برطرف کردن این مشکل، به‌روزرسانی امنیتی را روز دوشنبه برای ثابت‌افزارهای خود منتشر کرد. این شرکت اعلام کرده بررسی‌های خود را ادامه داده و هر محصول دیگری که تحت تأثیر این دربِ پشتی قرار گرفته باشد را وصله خواهد کرد.

یک محقق امنیتی مستقل این دربِ پشتی را در محصولات این شرکت کشف کرده و با استفاده از کد اثبات مفهومی، یک حمله خودکار علیه فهرست رایانامه‌ی Full Disclosure انجام داد. این محقق امنیتی به دستور شرکت Dahua این کد اثبات مفهومی را حذف کرده ولی اعلام کرده پس از گذشت 30 روز، زمانی‌که شرکت این دربِ پشتی را وصله کند، آن را منتشر خواهد کرد. این محقق اعلام کرد برای افشای آسیب‌پذیری به شرکت‌ها، سیاست‌های مخصوص خود را دارد.

این دربِ پشتی که شرکت Dahua از آن به‌عنوان یک آسیب‌پذیری یاد می‌کند، در محصولات مختلف این شرکت از جمله دوربین‌های IP و DVR ها وجود دارد. این شرکت روز دوشنبه در نامه‌ای به مشتریان و شرکای خود اعلام کرد، بخشی از کد محصولات خود را که منجر به بهره‌برداری از این آسیب‌پذیری می‌شد ایزوله کرده و در تلاش است هرچه سریع‌ترین وصله‌ای را برای محصولات خود منتشر کند. در این نامه، شرکت تأثیرات این دربِ پشتی را کم‌اهمیت جلوه داده و اعلام کرده این دربِ پشتی در اثر یک حمله‌ی سایبری با اهداف مخرب نصب نشده است.

محقق امنیتی ادعا می‌کند، یک مدیر غیرمجاز از راه دور و از طریق وب می‌تواند به دستگاه آسیب‌پذیر دسترسی داشته باشد. اگر مهاجم به یک آدرس URL خاص دسترسی داشته باشد، به‌راحتی می‌تواند نام مدیر را تغییر داده و یا حساب جدید ایجاد کند. مهاجم همچنین می‌تواند گذرواژه‌ی دستگاه را تغییر دهد. این محقق امنیتی مدعی است نفوذگران می‌توانند پرونده‌های پیکربندی و پایگاه داده‌ی موجود بر روی دستگاه را بارگیری کرده و به نام‌ها و گذرواژه‌های کاربران دستگاه دست یافته و از راه دور وارد حساب‌ها شده و دستگاه را کنترل کنند.

تاکنون تعداد دستگاه‌هایی که تحت تأثیر این دربِ پشتی قرار گرفته‌اند اعلام نشده است. این شرکت برای 11 مدل دستگاه، به‌روزرسانی برای ثابت‌افزارها منتشر کرده است ولی تخمین زده می‌شود تعداد مدل‌هایی که تحت تأثیر قرار گرفته‌اند خیلی بیشتر باشد. اگر آن‌طور که این محقق امنیتی ادعا می‌کند بهره‌برداری از این دربِ پشتی آسان باشد، مهاجمان می‌توانند از این دستگاه‌ها در بات‌نت‌هایی مانند Mirai استفاده کنند.

بات‌نت Mirai دستگاه‌های اینترنت اشیاء با پیکربندی‌های

امنیتیِ ضعیف را هدف قرار داده و بر روی چندین سرویس و وب‌گاه بزرگ در چند ماه گذشته، حمله‌ی منع سرویس توزیع‌شده انجام داده است. تعداد این حملات از زمانی‌که کد منبع این بدافزار به‌طور عمومی منتشر شد، افزایش چشمگیری داشته است. آزمایشگاه کسپرسکی ماه گذشته گزارش داد که نمونه‌ی لینوکسی این باتنت نیز با استفاده از باتنت‌های ویندوزی در حال توزیع است.

مدیریت امنیت

بزرگ‌ترین سازنده‌ی کارت‌های اعتباری در آمریکا، در حال بررسی یک نقض داده است

شرکت Verifone که بزرگ‌ترین سازنده‌ی پایانه‌های کارت‌های اعتباری در آمریکا است، وقوع یک نقض داده را در شبکه‌ی داخلی رایانه‌های خود بررسی می‌کند. گفته می‌شود این شبکه خصوصی است و ارتباطی با پایانه‌های کارت‌های اعتباری که این شرکت تولید می‌کند ندارد.

در وبلاگ برایان کربس، محقق امنیتی مشهور اعلام شده این شرکت رایانامه‌ای را به تمامی کارکنان و پیمانکاران خود ارسال کرده و از آن‌ها خواسته در عرض 24 ساعت گذرواژه‌ی حساب‌های خود را تغییر دهند. در این رایانامه یادآوری شده که مسئله‌ی اصلی در دست بررسی است و این اقدام تغییر گذرواژه‌ها، یک عمل محتاطانه است. متن رایانامه نشان می‌دهد کارکنان این شرکت از این پس نمی‌توانند اقدام به نصب برنامه بر روی رایانه‌ها و یا لپ‌تاپ‌های شرکت بکنند چرا که از این طریق امکان نصب بدافزارها فراهم شده و شبکه‌ی داخلی شرکت در معرض خطر قرار خواهد گرفت.

سخنگوی Verifone گفت: «در ماه ژانویه‌ی سال 2017، گروه امنیتی ما شواهدی مبنی بر یک نفوذ کوچک به شبکه‌ی داخلی را مشاهده کرد. شبکه‌ی سرویس‌های پرداخت ما تحت تأثیر این حمله‌ی سایبری قرار نگرفته است. ما هرچه سریع‌تر داده‌هایی که هدف حمله قرار گرفته‌اند را مشخص کرده و اقدامات پیشگیرانه را انجام خواهیم داد. ما حدس می‌زنیم به دلیل اقدامات سریع ما، ابعاد این حمله بسیار محدود شد.»

به نظر می‌رسد شرکت Verifone یادداشتی از طرف شرکت‌های کارت‌های اعتباری مانند ویزا و Mastercard دریافت کرده و از این نقض مطلع شده است. منابع ناشناس در یک پست وبلاگی گفتند این نفوذ واحد پشتیبانی از مشتریان را تحت تأثیر قرار داده که راه‌حل‌های پرداخت را برای ایستگاه‌های نفت و گاز فراهم می‌کند. این منبع ناشناس همچنین اعلام کرده یک گروه نفوذ روسی که به حمله علیه ارائه‌دهندگان سرویس‌های پرداخت مشهور است، این نقض داده را انجام داده است. مشکل اصلی این است که عوامل این گروه، برای نفوذ به شبکه‌ی این شرکت باید از اواسط سال 2016 میلادی در داخل شبکه‌ی Verifone بوده باشند.

با توجه به ماهیت این شرکت و این مسئله که نفوذگران داخل شبکه بوده‌اند، به‌نظر می‌رسد شرایط طوری که Verifone اعلام کرده خوب و خوش نیست. این شرکت از اعلام اطلاعات دقیق در مورد این نقض داده امتناع می‌کند تا وجهه‌ی خوب خود را بین مشتریان حفظ کند.

از هر 5 وب‌گاه، یک مورد همچنان از SHA-1 استفاده می‌کند

تقریباً 2 ماه است که بسیاری از مراکز صدور گواهی‌نامه از تابع درهم‌سازی SHA-1 برای صدور گواهی‌نامه استفاده نمی‌کنند. با این حال براساس بررسی‌هایی که شرکت امنیتی Venafi انجام داده، در سراسر جهان از هر 5 وب‌گاه، 1 مورد از گواهی‌نامه‌های SHA-1 استفاده می‌کنند.

علاوه بر اینکه بیشتر مراکز صدور گواهی دیگر گواهی‌نامه‌های SHA-1 را تولید نکرده و به سمت گواهی‌نامه‌های قوی‌تر SHA-2 حرکت کرده‌اند، بسیاری از تولیدکننده‌های مرورگر مانند مایکروسافت، گوگل و موزیلا نیز دیگر از گواهی‌نامه‌های SHA-1 پشتیبانی نمی‌کنند. حتی شرکت فیس‌بوک نیز اعلام کرده می‌خواهد گواهی‌نامه‌های SHA-1 را کنار بگذارد.

این شرکت امنیتی تقریباً 33 میلیون آدرس IP عمومی متعلق به وب‌گاه‌های مختلف را مورد بررسی قرار داده است. نتایج نشان می‌دهد بیش از 21 درصد از وب‌گاه‌های جهان، هنوز هم از گواهی‌نامه‌های SHA-1 استفاده می‌کنند. هرچند در حالت کلی وضعیت نسبت به پاییز سال قبل بسیار بهتر شده است (در سال قبل 35 درصد از کل وب‌گاه‌ها از SHA-1 استفاده می‌کردند) ولی اخیراً مشاهده کردیم که این تابع درهم‌سازی به‌طور رسمی شکسته شد.

چندین سال بود که گفته می‌شد تابع SHA-1 در برابر حمله‌ی تصادم آسیب‌پذیر است تا اینکه اخیراً شکسته شدن این الگوریتم به‌طور عملیاتی اثبات شد. نکته‌ای که برای محققان امنیتی بسیار عجیب بود این است که باوجود مشاهده‌ی عملیِ این حمله، مدیران وب‌گاه‌ها هرچه سریع‌تر به سمت استفاده از SHA-2 یا SHA-3 حرکت نمی‌کنند. محققان احتمال می‌دهند این مدیران نمی‌دانند که وب‌گاه‌هایشان در معرض خطر قرار دارد.

استفاده از گواهی‌نامه‌های SHA-1 علاوه بر اینکه وب‌گاه‌ها و کاربران را در معرض آسیب‌پذیری و خطر قرار می‌دهد، تجربه‌ی نامناسبی از مرور وب را نیز به دنبال خواهد داشت چرا که مرورگرها دیگر از SHA-1 پشتیبانی نکرده و هنگام مواجهه با وب‌گاه‌های ناامن به کاربران هشدار خواهند داد.

مدیریت امنیت

کریس ویکری اعلام کرد یک نقض داده‌ی عظیم را کشف کرده است

محقق امنیتی معروف با نام کریس ویکری اعلام کرد هرچه سریع‌تر منبع یک نقض داده‌ی بزرگ را نشان خواهد داد که افراد زیادی را تحت تأثیر قرار داده است. او در تیزری این نشت داده را اطلاع‌رسانی کرد و تعداد شناسه‌های در معرض خطر را 30 هزار شناسه عنوان کرد. محققان امنیتی در تلاش هستند تا نام قربانیِ این نقض داده را حدس بزنند. باتوجه به اینکه حجم این نقض داده بسیار وسیع گزارش شده، نامزدهای محدودی برای قربانی بودن وجود دارد. در فضای مجازی نام شرکت Aadhaar به‌عنوان قربانی این حادثه‌ی سایبری در حال چرخش است.

این شرکت بزرگ‌ترین ارائه‌کننده‌ی سامانه‌های شناسه‌ی بیومتریک است که از تاریخ 8 اسفند ماه تاکنون بیش از 1.123 میلیارد نفر در این سرویس ثبت‌نام کرده‌اند. این پایگاه داده حاوی اطلاعات بیش از 99 درصد از افراد بالای 18 سال در هندوستان است. دولت هندوستان به‌سرعت اعلام کرد که این نقض داده در سامانه‌ی Aadhaar رخ نداده است.

یکی دیگر از فرضیه‌ها در مورد منشأ این نقض داده‌ی بزرگ، کشور چین است. چین تنها کشوری است که پایگاه داده‌ای گسترده و بزرگ شامل هویت و شناسه‌ی افراد این کشور دارد. اگر بخواهیم به شرکت‌های بخش خصوصی توجه کنیم، شرکت‌های محدودی وجود دارند که دارای پایگاه داده‌ای عظیم هستند. از جمله‌ی این شرکت‌ها می‌توان فیس‌بوک، واتس‌اپ، اپل، مایکروسافت، یاهو، شرکت چینی WeChat و شبکه‌ی اجتماعی Qzone را نام برد.

کریس ویکری قبلاً نیز پایگاه داده‌های بزرگی که به شکل باز در سطح اینترنت قابل دسترسی بودند، کشف کرده است. در سال 2015 میلادی او 191 میلیون رکورد اطلاعاتی مربوط به رأی‌دهندگان در آمریکا را کشف کرد. در سال 2016 او 132 گیگابایت پایگاه داده‌ی MongoDB را کشف کرد که بدون حفاظت در سطح اینترنت قرار گرفته بودند. او همچنین اطلاعات رأی‌دهندگان مکزیکی بالغ بر 93.4 میلیون رکورد را کشف کرده است.

مدیریت امنیت

از کار افتادن سرویس میزبانی Freedom و کاهش تعداد وب‌گاه‌ها در وب تاریک

پس از وقوع یک حمله‌ی سایبری علیه ارائه‌دهنده‌ی سرویس میزبانی Freedom Hosting II، تعداد سرویس‌های مخفی در وب تاریک بسیار کاهش یافته است. گفته می‌شود این ارائه‌دهنده 20 درصد از سرویس‌های موجود در وب تاریک را میزبانی می‌کرد.

سرویس Freedom Hosting II تقریباً از 11 هزار وب‌گاه میزبانی می‌کرد و ماه گذشته توسط نفوذگران ناشناس از کار افتاد. نفوذگران پس از اینکه مشاهده کردند این سرویس بیشتر برای وب‌گاه‌های پورنوگرافی کودکان مورد استفاده قرار می‌گیرد، آن را از حالت برخط خارج کردند. این نفوذگران همچنین رکوردهایی بالغ بر اطلاعات 380 هزار کاربر را افشاء کردند.

سرویس OnionScan یک ابزار متن‌باز برخط برای پویش و بررسی وب تاریک است. تجزیه و تحلیلی که با استفاده از این ابزار انجام شده نشان می‌دهد، از 30 هزار سرویس مبتنی بر Tor، تنها 4400 سرویس برخط باقی مانده است. مسئول پروژه‌ی OnionScan می‌گوید: «این 4400 سرویس برخط بسیار کمتر از پویش قبلی است. ما معتقدیم که از کار افتادن Freedom Hosting II تنها باعث حذف هزاران وب‌گاه در وب تاریک نشده است بلکه سایر ارائه‌دهندگان سرویس میزبانی را نیز تحت تأثیر قرار داده است.»

محققان امنیتی معتقدند کاهش تعداد وب‌گاه‌ها در وب تاریک می‌تواند نتیجه‌ی ناپدید شدن سرویس رایانامه‌ی Sigaint نیز باشد. این سرویس بدون هیچ‌گونه هشداری به کاربران از حالت برخط خارج شده است. براساس آخرین پویش OnionScan تقریباً 4 هزار درخواست HTTP در وب تاریک شناسایی شده است. در این پویش همچنین 250 سرویس TLS، 270 سرویس SSH، 220 گره بیت‌کوین، 100 سرویس SMTP و تعداد انگشت‌شماری سرویس FTP و VNC شناسایی شد.

این پویش نشان داد که هنوز هم در سطح وب تاریک برخی از سرویس‌ها به‌طور مناسب پیکربندی نشده‌اند و محققان توانستند به هزاران آدرس IP منحصربفرد مربوط به سرویس‌های مخفی و کارخواه‌های آن‌ها دست یابند. از زمان انتشار ابزار OnionScan چندین گزارش منتشر شده است. این ابزار قرار است در ادامه بهبود یافته و بیشتر مورد استفاده قرار بگیرد.

مدیریت امنیت

ربات‌ها در برابر حملات سایبری آسیب‌پذیر هستند

نرم‌افزارها و ثابت‌افزارهایی که در ربات‌ها مورد استفاده قرار می‌گیرند، در معرض آسیب‌پذیری‌های حیاتی قرار دارند و مهاجمان را قادر می‌سازند تا از راه دور کنترل ماشین را در دست بگیرند.

امروزه شاهد هستیم که تعداد ربات‌ها در خانه‌ها، مراکز تجاری، محیط‌های صنعتی، نظامی، قانونی و بخش بهداشت و سلامت رو به افزایش است. شرکت بین‌المللی داده تخمین زده است در سال 2020 مقدار هزینه‌ای که صرف ربات‌ها و سرویس‌های مربوط به آن‌ها خواهد شد، نزدیک به 188 میلیارد دلار است.

سال‌های گذشته شاهد بودیم که در اثر اتفاقاتی که برای ربات‌ها پیش آمده، چندین نفر زخمی یا کشته شدند. محققان امنیتی هشدار دادند اگر روند وجود آسیب‌پذیری در ربات‌ها افزایش یابد، شاهد موج جدیدی از اتفاقات ناگوار خواهیم بود. محققان امنیتی ربات‌های خانگی، صنعتی و تجاری را از 6 شرکت مختلف مورد بررسی قرار دادند. محققان به ربات‌های واقعی دسترسی نداشته و نرم‌افزارها، برنامه‌های تلفن همراه و ثابت‌افزارهای آن‌ها را تحلیل و آزمایش کردند.

کارشناسان امنیتی در نمونه‌های بررسی‌شده 50 آسیب‌پذیری مختلف را کشف کردند ولی اعلام شد که این تحلیل و بررسی خیلی عمیق نبوده و به احتمال زیاد، تعداد آسیب‌پذیری‌ها بسیار بیشتر است. محققان این آسیب‌پذیری‌ها را به شرکت‌های مربوطه گزارش کردند ولی فقط 4 شرکت به این گزارش‌ها پاسخ داده‌اند.

آسیب‌پذیری در ربات‌ها و تأثیرات آن

به گزارش محققان امنیتی، ربات‌هایی که مورد بررسی قرار گرفتند دارای آسیب‌پذیری‌ها و مشکلات متعددی بودند. از جمله‌ی این اشکالات می‌توان ایرادات در برقراری ارتباطات، احراز هویت، رمزنگاری، حریم خصوصی، پیکربندی‌های پیش‌فرض و مؤلفه‌های متن‌باز را نام برد. این آسیب‌پذیری‌ها به مهاجمان اجازه می‌دهد ارتباطات بین ربات و دستگاه کنترل‌کننده را شنود کنند، بدون نیاز به نام کاربری و گذرواژه به سرویس‌های حساس دسترسی داشته باشند، بر روی آن برنامه‌های مخرب نصب کنند و اطلاعاتی را که به‌درستی رمزنگاری نشده، استخراج کنند. محققان گفتند آسیب‌پذیری‌هایی که کشف کردند برای جاسوسی از طریق دوربین و میکروفن ربات، سرقت داده‌های شخصی و تجاری و در دست گرفتن کنترل ربات، قابل بهره‌برداری هستند. محققان اشاره کردند، شرکت‌های تولیدکننده‌ی ربات باید قبل از سرعت دادن به تولید و روانه‌ی این ماشین‌ها به بازار، بیشتر بر روی امنیت متمرکز شوند.

مدیریت امنیت

از آسیب‌پذیری Cloudbleed بهره‌برداری صورت نگرفته است

روز چهارشنبه، شرکت Cloudflare به مشتریان خود اطلاع داد از آسیب‌پذیریِ نشت حافظه که اخیراً کشف شده بود، قبل از وصله شدن، بهره‌برداری با اهداف مخرب صورت نگرفته است.

این آسیب‌پذیری در تاریخ 29 بهمن ماه توسط محققی از شرکت گوگل با نام تاویس اورماندی، کشف شد. این محقق امنیتی به‌خاطر شباهتی که این آسیب‌پذیری به HeartBleed داشت، آن را Cloudbleed نام‌گذاری کرد.

شرکت Cloudflare تشخیص داد که این آسیب‌پذیری باعث نشت حافظه شده و می‌تواند اطلاعات حساسی از جمله کوکی‌ها و رمزواره‌های احراز هویت را برای مهاجمان برگرداند. اورماندی همچنین کشف کرده اطلاعاتی که لو می‌رود حاوی گذرواژه‌ها، کلیدهای رمزنگاری، پیام‌های خصوصی، آدرس‌های IP و درخواست‌های HTTP است.

این آسیب‌پذیری در سپتامبر سال 2016 میلادی معرفی شد ولی تأثیر جدی آن در ماه فوریه بود زمانی که از هر 3.3 میلیون درخواست Cloudflare، یک مورد باعث نشت اطلاعات می‌شد. این آسیب‌پذیری در عرض چند ساعت وصله شد ولی به‌دلیل نشت اطلاعاتی که در حافظه‌ی نهان موتورهای جستجو وجود داشت، برطرف کردن آن چند روز زمان لازم داشت.

روز چهارشنبه در یک پست وبلاگی، مدیرعامل این شرکت اعلام کرد هرچند که این آسیب‌پذیری بسیار جدی بود و تأثیرات گسترده و وسیعی داشت، بررسی‌ها نشان داد که شواهدی مبنی بر بهره‌برداری با اهداف مخرب وجود ندارد. او همچنین اعلام کرد بخش عمده‌ای از مشتریان، تحت تأثیر این آسیب‌پذیری قرار نگرفته‌اند.

مدیرعامل Cloudflare گفت: «اگر نفوذگری قبل از وصله شدن آسیب‌پذیری از آن مطلع می‌شد و از آن بهره‌برداری می‌کرد، باید درخواست‌های زیادی را به سمت صفحات حاوی این داده‌ها ارسال می‌کرد تا از این آسیب‌پذیری بهره‌برداری کند. همچنین آن‌ها در ادامه باید نتایج خود را ثبت می‌کردند. در این سناریو ممکن بود بسیاری از اطلاعات به‌دردنخور باشد ولی بخش کوچکی از آن می‌توانست حاوی داده‌های حساس و مهم باشد.»

او افزود: «سناریویی که برای ما بسیار وحشتناک است این است که نفوذگری قبل از اینکه گوگل این آسیب‌پذیری را به ما اطلاع دهد، از آن باخبر شده و در خفاء از آن بهره‌برداری کرده باشد.» بررسی‌های Cloudflare در خصوص این آسیب‌پذیری همچنان ادامه دارد و نتایج نشان می‌دهد نمونه‌ای از نشت اطلاعات حساس مانند گذرواژه‌ها، شماره کارت‌های پرداخت، کلیدهای رمزنگاری و رکوردهای سلامت و بهداشت وجود ندارد.

مدیرعامل Cloudflare گفت: «این قضیه درست نیست که نتیجه‌گیری کنیم گذرواژه‌ها، کلیدهای رمزنگاری و شماره کارت‌های پرداخت در معرض خطر قرار گرفته است. با این‌حال اگر داده‌ای در معرض خطر قرار گرفته، این نشت اطلاعات گسترده نیست. ما هیچ گزارش تأییدشده‌ای

مبنی بر مشاهده‌ی اطلاعات حساس کاربران در صفحات ذخیره‌شده در حافظه‌ی نهان را از طرف نهادهای ثالث دریافت نکرده‌ایم.»

برای کاربرانی که نگران هستند داده‌های آن‌ها در معرض خطر قرار گرفته باشد، فهرستی از وب‌گاه‌هایی که تحت تأثیر قرار گرفته‌اند و یک برنامه‌ی ساده‌ی کروم برای سامانه‌ی مک قابل دسترسی است.

ASADAL INTERNET, INC. started its business in Seoul Korea in February 1998 with the fundamentalgoal of providing better internet services to the world. ASADAL stands for the "morning land" in ancient Korean. Asadal has about 35 staffs including well experienced web designers, programmers, and server engineers.

مدیریت امنیت

بدافزار کشف‌نشده‌ی مک در وب تاریک به قیمت ۴۰ بیت‌کوین به‌فروش می‌رسد

نفوذگران در حال حاضر در وب تاریک بدافزاری مخصوص سامانه‌های مک را به‌فروش می‌رسانند. این بدافزار تاکنون شناسایی نشده و به نفوذگران این امکان را می‌دهد بدون اینکه توسط محصولات امنیتی شناسایی شوند، کنترل کامل دستگاه MacOS را در دست گیرند.

این بدافزار با نام Proton یک ابزار مدیریت از راه دور است که در حال حاضر در بازارهای زیرزمینی روسیه به فروش می‌رسد. قیمت اولیه‌ی این بدافزار 100 بیت‌کوین بوده که اگر با قیمت فعلی بیت‌کوین در نظر بگیریم، ارزشی بالغ بر 100 هزار دلار داشته است ولی در حال حاضر این بدافزار به قیمت 40 بیت‌کوین فروخته می‌شود. اگر نفوذگر بخواهد بدافزار را تنها بر روی یک سامانه‌ی مک نصب کند، می‌تواند آن را با قیمت 20 بیت‌کوین خریداری کند.

این بدافزار، کنترل کامل دستگاه قربانی را در اختیار نفوذگر قرار می‌دهد. این کنترل می‌تواند شامل کی‌لاگر، نظارت‌ها با استفاده از وب‌کم و میکروفون، بارگذاری و بارگیری پرونده و سایر عملیات باشد. هر موقع که بر روی دستگاه داده‌ی جدیدی وارد می‌شود، به نفوذگر اعلام خواهد شد.

بدافزار Proton یک تهدید واقعی برای سامانه عامل مک محسوب می‌شود چرا که با امضای اصلی اپل در وب تاریک به فروش می‌رسد و حمله‌ای بسیار پیچیده را انجام می‌دهد. در گزارش‌های مربوط به این بدافزار می‌خوانیم: «نویسنده‌ی بدافزار Proton به نحوی بسیار دقیق از فرآیند مسدودسازی اپل استفاده کرده و از گواهی‌نامه‌های اصلی و معتبر اپل در حمله‌ی خود بهره برده است. محققان امنیتی حدس می‌زنند توسعه‌دهنده‌ی بدافزار احتمالاً شناسه‌ی توسعه‌دهندگان در سرویس اپل را برای ثبت‌نام جعل کرده یا از گواهی‌نامه‌های سرقتیِ سایر توسعه‌دهندگان برای این منظور استفاده کرده است.»

به نظر می‌رسد یک آسیب‌پذیری روز-صفرم که قبلاً وصله نشده بود، به این بدافزار کمک می‌کند تا بر روی سامانه‌ی مک به دسترسی ریشه برسد. محققان امنیتی معتقدند نویسنده‌ی این بدافزار از قبل اطلاعات مربوط به این آسیب‌پذیری را می‌دانسته و نزد خود نگه داشته و آن را به اشتراک نگذاشته است.

محققان امنیتی می‌گویند: «40 بیت‌کوین برای نصب نامحدود این بدافزار و دسترسی به کد منبع آن هنوز هم مقدار بسیار بالایی محسوب می‌شود. به‌طور معمول بدافزارهای مختلفی برای سامانه‌های مک به‌صورت رایگان نیز وجود دارند. این قیمت شاید باعث شود تا توزیع این بدافزار محدود شود و تشخیص آن با استفاده از نرم‌افزارهای امنیتی سخت باشد. هرچند بدافزار Proton در انجمن‌های وب تاریک به فروش می‌رسد ولی در یوتیوب

نیـز تبلیـغ شـده و دارای یـک وب‌گاه عمومـی نیـز هسـت. ایـن بدافـزار ممکـن اسـت بیـش از چیـزی کـه نویسـنده انتظـار دارد، بـا اسـتقبال نفوذگـران مواجـه شـود.»

ASADAL INTERNET, INC. started its business in Seoul Korea in February 1998 with the fundamentalgoal of providing better internet services to the world. ASADAL stands for the "morning land" in ancient Korean. Asada has about 35 staffs including well experienced web designers, programmers, and server engineers.

مدیریت امنیت

در سرویس‌های مایکروسافت آسیب‌پذیری کشف کنید، دو برابر جایزه بگیرید!

مایکروسافت اعلام کرد برای دو ماه آینده، هر محقق امنیتی که آسیب‌پذیری را از طریق سرویس برنامه‌ی پاداش در ازای اشکال این شرکت گزارش کند، پاداشی دو برابر مقدار قبل دریافت خواهد کرد. از تاریخ 11 اسفند تا 11 اردیبهشت ماه، هر آسیب‌پذیری که بر روی پورتال آفیس 365 مایکروسافت و Microsoft Exchange Online کشف شود، پاداشی دو برابر مقدار فعلی به آن تعلق خواهد گرفت.

محققان امنیتی که علاقه‌مند هستند در این بازه‌ی دو ماهه، دو برابر پاداش دریافت کنند، می‌توانند بر روی 6 دامنه‌ی این شرکت به کشف آسیب‌پذیری بپردازند. این دامنه‌ها عبارتند از: portal.office.com، outlook.office.com، *.outlook.com و office365.com، outlook.com.

مایکروسافت از سپتامبر سال 2014 میلادی، برنامه‌ی پاداش در ازای اشکال را به‌طور برخط آغاز کرده و در سال 2015، ویژگی‌های آفیس 365 و Azure را به این برنامه اضافه کرده است. سال گذشته نیز این شرکت، وان‌درایو را نیز به این برنامه اضافه کرد.

این شرکت به‌طور معمول به هر آسیب‌پذیری که توسط این سرویس برخط گزارش شود، مبلغ 500 تا 1500 دلار پاداش می‌دهد ولی برای آسیب‌پذیری‌هایی که در دو ماه آینده گزارش شود، مبلغی بین 1000 تا 3000 دلار پاداش تعلق خواهد گرفت. برای تمامی آسیب‌پذیری‌هایی که در فهرست این برنامه اعلام شده، پاداش بیشتری در نظر گرفته شده است.

مایکروسافت در پورتال برنامه‌ی پاداش در ازای اشکال خود، آسیب‌پذیری‌های واجد شرایط دریافت پاداش را فهرست کرده است. این آسیب‌پذیری‌ها عبارتند از XSS، CSRF، دسترسی و تغییر داده‌ها بدون احراز هویت، ارجاع مستقیم به اشیاء به‌صورت ناامن، آسیب‌پذیری‌های تزریق، احراز هویت، اجرای کد در سمت کارگزار، ارتقاء امتیازات، پیکربندی‌های اشتباه.

مسئولان بخش امنیتی مایکروسافت در یک پست وبلاگی توضیح دادند: «ما متوجه شدیم که محققان امنیتی علاقه دارند سرویس‌های ما را از لحاظ امنیتی آزمایش کنند تا به راه‌حل‌های ما اعتماد کنند. ما همچنین معتقدیم اگر یکی از کاربران آسیب‌پذیری را در سرویس آفیس 365 به ما گزارش دهد، ما باید به‌طور کامل از او حمایت کنیم. این گزارش‌های خارجی و تلاش‌هایی که گروهِ امنیت داخلی ما انجام می‌دهد، باعث می‌شود سرویس‌های امن‌تری را به کاربران خود ارائه کنیم.»

مدیریت امنیت

شرکت ارسال‌کننده‌ی هرزنامه، ۱,۴ میلیارد رکورد متعلق به کاربران را لو داد

یک شرکت که با استفاده از دو ارسال‌کننده‌ی هرزنامه‌ی معروف کار می‌کند، یک سری پرونده حاوی اطلاعات مهم و حساس متعلق به این شرکت را لو داد. گفته می‌شود در این پرونده‌های حساس بالغ بر 1.4 میلیارد رکورد متعلق به کاربران وجود داشت.

شرکت RCM که مدعی است در حوزه‌ی بازاریابی مشروع فعالیت می‌کند، توسط دو ارسال‌کننده‌ی هرزنامه مدیریت می‌شود. محقق امنیتی، کریس ویکری که قبلاً حجم وسیعی از پایگاه داده‌های محافظت‌نشده را در سطح اینترنت کشف کرده و از این طریق برای خود اسم و رسمی بهم زده بود، امروز از یک نقض داده‌ی گسترده خبر داد. اینک شواهد نشان می‌دهد نقض داده در پایگاه داده‌ی این شرکت تبلیغاتی رخ داده است.

داده‌های لورفته توسط ویکری مورد بررسی قرار گرفته است و بخشی از پرونده‌های لورفته به مراجع قضایی و قانونی ارائه شده تا اثبات شود یک رخداد غیرقانونی بوقوع پیوسته است. گزارش این نقض داده به شرکت‌های بزرگ فناوری همچون مایکروسافت و اپل نیز ابلاغ شده است.

به گزارش ویکری در داده‌های لورفته، اسناد، پرونده‌های پشتیبان و رکوردهای ثبت‌شده از گفتگوها وجود دارد. یکی از مهم‌ترین پرونده‌ها، پایگاه داده‌ای شامل 1.3 میلیارد رکورد مربوط به کاربران است که در آن نام، آدرس رایانامه، آدرس فیزیکی و IP کاربران ذخیره شده است.

این کارشناس امنیتی معتقد است مقدار زیادی از این داده‌ها معتبر بوده و ارسال‌کنندگان هرزنامه این اطلاعات را از طریق چک‌های اعتباری، قرعه‌کشی‌ها و فرصت‌های آموزشی جمع‌آوری کرده‌اند. ویکری معتقد است داده‌هایی که در معرض خطر قرار گرفته‌اند می‌توانند منجر به سقوط امپراطوری این ارسال‌کننده‌ی هرزنامه شود. در بین داده‌های لورفته اطلاعاتی مبنی بر استفاده‌ی این شرکت از ابزارهای غیرقانونی نیز به چشم می‌خورد. به‌عنوان مثال، در یکی از این پرونده‌ها روشی توضیح داده شده که برای هدف قرار دادن کارگزارهای جی‌میل مورد استفاده قرار می‌گیرد. در این روش تلاش می‌شود با باز کردن تعداد زیادی ارتباط بین کارگزارهای گوگل، از آن‌ها برای توزیع هرزنامه استفاده شود.

فصل سوم

امنیت سایبری

امنیت‌سایبری

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، Soundcloud، Splitwise، Trello 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.

آمازون در ادامه افزود: «به‌دلیل اینکه در چند سال اخیر، سامانه‌های S3 آمازون رشد چشمگیری داشتند، راه‌اندازی مجدد آن‌ها و بررسی‌های امنیتی برای اعتبارسنجی و صحت آن‌ها به زمان طولانی نیاز داشت.» آمازون از مشکلی که برای مشتریان پیش آمد عذرخواهی کرده است.

آمازون اعلام کرد پس از این اتفاق، چندین بهبود را در سامانه‌های خود اعمال کرده است به‌طور مثال بر روی وارد کردن ورودی‌های معتبر بررسی‌های بیشتری صورت می‌گیرد تا در آینده چنین مشکلاتی رخ ندهد.

امنیت‌سایبری

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.

امنیت‌سایبری

ارائه‌دهنده‌ی معروف سرویس رایانامه در شبکه‌ی گمنامی Tor، از دسترس خارج شده است

ارائه‌دهنده‌ی سرویس رایانامه در شبکه‌ی Tor با نام SIGAINT برای سومین هفته‌ی متوالی از دسترس خارج شده و هنوز علت این ماجرا به‌طور رمزآلودی پنهان مانده است. SIGAINT یکی از معروف‌ترین سرویس‌های رایانامه‌ی وب در شبکه‌ی Tor است که برای ارسال رایانامه‌ها توسط کاربران با حفظ گمنامی، مورد استفاده قرار می‌گیرد.

این سرویس به‌رغم تمام تلاش‌های مراجع قضایی برای شناسایی کاربران، سال‌ها به فعالیت خود ادامه داده بود. این سرویس به‌طور مداوم تحت حمله‌ی نهادهای دولتی قرار می‌گرفت به‌طوری که در سال 2015 میلادی، مدیر این سرویس به کاربران هشدار داد که مراجع قانونی در تلاش هستند با نفوذ به این سرویس، گمنامی کاربران را زیر سؤال برده و آن‌ها را شناسایی کنند.

به گزارش مدیر این سرویس در سال 2015، حمله‌ی مداومی با دسترسی به 6 درصد از گره‌ها در شبکه‌ی Tor (نزدیک به 70 گره خروجی Tor) تلاش داشت تا این سرویس رایانامه را از کار بیندازد. یکی از مدیران SIGAINT تأیید کرد که کارگزارهای این سرویس توسط 58 گره مخرب و خروجی Tor هدف قرار گرفته است ولی یکی از اعضای پروژه‌ی Tor تعداد 12 گره خروجی دیگر را نیز کشف کرد.

اینک این ارائه‌دهنده‌ی سرویس رایانامه، حداقل از تاریخ 23 بهمن ماه از کار افتاده است و از اینکه چه اتفاقی برای این سرویس افتاده، خبری در دست نیست. البته شایعات مختلفی در فضای مجازی در حال پخش شدن است.

با این حال اگر این سرویس هم از کار افتاده باشد، در سطح شبکه‌ی Tor چندین ارائه‌دهنده‌ی سرویس رایانامه وجود دارد. از جمله این سرویس‌ها می‌توان RuggedInbox، Torbox، Bitmessage، Mail2Tor، RiseUp، AnonInbox، Autistici، Lelantos و VFEMail را نام برد.

امنیت‌سایبری

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.

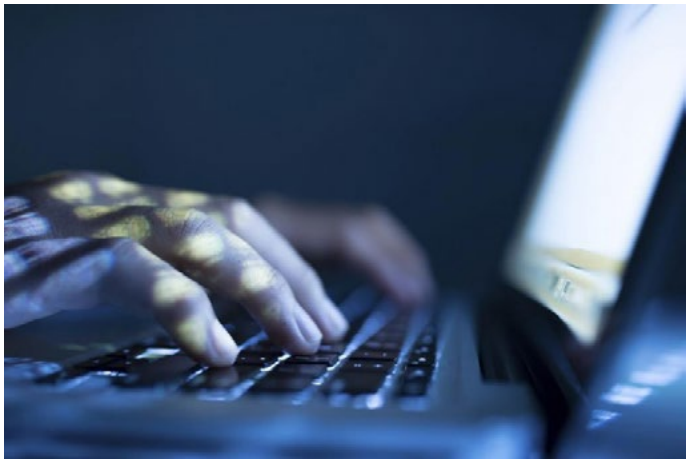
در این پرونده‌ها چه چیزی وجود دارد؟ ویکی‌لیکس مدعی شده سازمان سیا دارای نرم‌افزاری است که به این سازمان امکان می‌دهد بر روی دستگاه‌های الکترونیکی مدرن از جمله آیفون، دستگاه‌های اندرویدی، رایانه‌ها و تلویزیون‌های هوشمند کنترل کامل داشته باشند.

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.

امنیت‌سایبری

یک میلیون گذرواژه‌ی رمزگشایی‌شده‌ی یاهو و جی‌میل در وب تاریک به فروش می‌رسد



در چند وقت اخیر روزی را پشت سر نمی‌گذاریم که در آن خبری از یک نقض داده وجود نداشته باشد. سال گذشته میلیاردها حساب کاربری بر روی وب‌گاه‌ها و سرویس‌های معروف مانند یاهو، لینکدین، جی‌میل تامبلر در سطح اینترنت در معرض خطر قرار گرفت.

خبرها حاکی از آن است که گذرواژه‌های ورود و اطلاعات شخصی افراد در قالب 1 میلیون حساب کاربری متعلق به یاهو و جی‌میل در وب تاریک به فروش می‌رسد. حساب‌هایی که در بازارهای وب تاریک به فروش می‌رسند حاوی اطلاعاتی مانند نام کاربری، آدرس رایانامه و گذرواژه‌ی کاربران به شکل متن ساده است.

حساب‌هایی که برای فروش گذاشته شده متعلق به یک نقض داده‌ی واحد نبوده و از چندین حمله‌ی سایبری بزرگ ایجاد شده است. نفوذگری با شناسه‌ی SunTzu583 در بازار وب تاریک، این حساب‌ها را برای فروش قرار داده است.

داده‌هایی که توسط SunTzu583 به فروش می‌رسد به‌طور مستقل توسط خبرگزاری‌های معتبرِ نفوذ تأیید نشده ولی برخی از سامانه‌های اطلاع‌رسانی نقض داده مانند Hacked-DB و HaveIBeenPwned اعلام کردند این اطلاعات با داده‌هایی که آن‌ها از چند نقض داده منتشر کرده بودند، مطابقت دارد.

با این شرایط دیگر نیازی به گفتن نیست که شما باید گذرواژه‌ی تمامی حساب‌های کاربری خود را تغییر دهید. به‌سرعت بر روی حساب‌های خود ویژگی احراز هویت دوعاملی را فعال کنید. مجدداً تکرار و قویاً توصیه می‌کنیم: از یک گذرواژه‌ی یکسان بر روی چند حساب کاربری استفاده نکنید.

هرچند ماه یک‌بار گذرواژه‌های خود را تغییر دهید تا بازه‌ی استفاده از آن برای نفوذگران محدود شود. اگر به‌خاطر سپردن یک گذرواژه‌ی سخت برای هر حساب کاربری برای شما مشکل است، از یک برنامه‌ی مدیریت گذرواژه استفاده کنید. این برنامه به شما امکان می‌دهد برای هر حساب یک گذرواژه‌ی منحصربفرد و قوی تولید و ذخیره کنید.

امنیت‌سایبری

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 نفوذEquation 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.

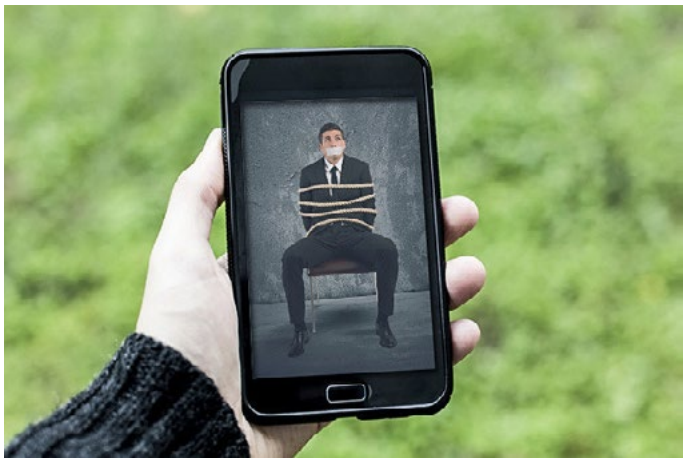
یکی از کاربران شرکت‌کننده در بحث گفته است: «استفاده از کد مشترک بزرگ‌ترین عاملی بوده که به کسپرسکی اجازه داده تمامی این بدافزارها را به یک گروه نسبت دهد. خرید و استفاده از دامنه‌های دستور و کنترل، دومین اشتباه مسلم NSA بوده است چرا که در بررسی‌ها، بیشترین بخشی که مورد تحلیل و بررسی قرار می‌گیرد، این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

پس از اینکه ویکی‌لیکس قابلیت‌های نفوذ سازمان سیا را منتشر کرد، شرکت‌های امنیتی ارزیابی‌های خود را شروع کردند. ویکی‌لیکس هیچ بهره‌برداری را منتشر نکرده و این مسئله باعث شده تا تشخیص اینکه سازمان سیا واقعاً چه کارهایی می‌تواند انجام دهد، سخت باشد. با این‌حال، در نگاه اول به‌نظر نمی‌رسد ابزارهای نفوذ این آژانس اطلاعاتی بسیار پیچیده باشد.

امنیت‌سایبری

سناتورهای دموکرات پنسیلوانیا هدف حملات باج‌افزارها قرار گرفتند



حرب دموکرات پنسیلوانیا با یک حمله‌ی باج‌افزاری مواجه شده که پرونده‌های 16 سناتور را رمزنگاری کرده است. این حمله صبح روز جمعه کشف شد و در حال حاضر نیز وب‌گاه این حزب از حالت برخط خارج است و بر روی آن پیغام «خطا در برقراری ارتباط با پایگاه داده» نمایش داده می‌شود. هنگام بازدید از صفحات سناتورها نیز این پیغام خطا نمایش داده می‌شود.

در بیانیه‌ی متنی این حزب آمده است: «مقامات انجمن با مراجع قانونی در تماس هستند تا این ماجرا را پیگیری کنند و مایکروسافت با این حزب همکاری دارد تا سامانه‌ها و زیرساخت‌های فناوری اطلاعات را بازیابی کنند.» این بیانیه به‌طور متنی منتشر شده چرا که این حزب در حال حاضر نمی‌تواند از سرویس رایانامه‌ی خود استفاده کند. در بیانیه ذکر شده: «هنوز مدرکی مبنی بر هدف قرار گرفتن سامانه‌های این حزب و آلوده شدن داده‌های آن مشاهده نشده است.»

دفتر حزب دموکرات روز جمعه باز بود ولی هیچ‌کس نمی‌توانست به داده‌ها و شبکه دسترسی داشته باشد.

هنگامی که روز جمعه این اتفاق در خبرگزاری‌ها منتشر شد، سخنگوی FBI اعلام کرد این موضوع باید بررسی شود و روز شنبه این حمله تأیید شده و اعلام کردند تعدادی از سناتورهای این حزب، تحت تأثیر این حمله‌ی سایبری قرار گرفته‌اند.

سناتورهای جمهوری‌خواه پنسیلوانیا دارای شبکه‌ی جداگانه‌ای هستند که تحت تأثیر این حمله قرار نگرفته است. سامانه‌ی فرماندار این ایالت نیز که عضو حزب دموکرات است، از این شبکه جدا بوده و آسیب ندیده است. هرچند خیلی غیرعادی نیست که قربانیان، مقدار باج درخواستی از طرف مهاجمان را کم اعلام می‌کنند ولی سخنگوی این حزب اعلام نکرد آیا نسخه‌ی پشتیبان از داده‌ها وجود داشته است یا خیر؟

وقتی از سخنگوی حزب دموکرات پنسیلوانیا سؤال شد که آیا باج درخواستی را پرداخت می‌کنید یا خیر، او پاسخ داد در حال حاضر با شرکت مایکروسافت همکاری داریم تا ببینیم وضعیت فعلی ما چیست. باوجود تمام هشدارهایی که در مورد باج‌افزارها به کاربران داده می‌شود، هنوز هم شاهد هستیم که نهادهای دولتی، ادارات پلیس، بیمارستان‌ها و دانشگاه‌ها قربانی این نوع تهدیدات می‌شوند.

محققان امنیتی اشاره می‌کنند هیچ‌گاه نسخه‌ی پشتیبان را بر روی حافظه‌ی خارجی که به سامانه‌ی شما متصل است، ذخیره نکنید. بهترین گزینه این است که از روش 1-2-3 بهره ببرید. حداقل 3 رونویس از پرونده‌های خود تهیه کنید. این رونویس‌ها حداقل در 2 قالب متفاوت باشند و یکی از رونویس‌ها حتماً بر روی حافظه‌ی خارجی که متصل به سامانه و شبکه نیست نگهداری شود.

فصل چهارم

اخبار فنی

اخبار فنی

بستر HackerOne به پروژه‌های متن‌باز سرویس رایگان ارائه می‌دهد

ارائه‌دهنده‌ی بستر برنامه‌های پاداش در ازای اشکال، HackerOne روز پنج‌شنبه اعلام کرد پروژه‌های متن‌باز می‌توانند از سرویس‌های حرفه‌ای این بستر بدون هیچ هزینه‌ای استفاده کنند. بهره‌مندی از این سرویس‌ها در قبال داشتن یک سری شرایط مشخص فراهم خواهد شد. در خبرها شاهد بودیم HackerOne اخیراً توانسته است 40 میلیون دلار بودجه‌ی مالی جذب کند و در حال حاضر از 36 برنامه‌ی پاداش در ازای اشکال مربوط به پروژه‌ی متن‌باز از جمله گیت‌لب، روبی، ریل و دی‌جنگو میزبانی می‌کند. این شرکت امیدوار است بتواند سایر پروژه‌های متن‌باز را نیز به سمت بستر خود جذب کند.

در این برنامه، پروژه‌های متن‌باز می‌توانند به‌طور رایگان از سرویس‌های حرفه‌ای HackerOne استفاده کنند. این بستر سرویس‌هایی همچون ارسال آسیب‌پذیری، تحلیل آسیب‌پذیری‌ها، تشخیص گزارش‌های تکراری و پرداخت پاداش را به مشتریان خود ارائه می‌دهد.

نکته‌ای که لازم است اشاره کنیم این است که هرچند پروژه‌های متن‌باز می‌توانند بدون هیچ هزینه‌ای از این سرویس‌ها استفاده کنند ولی اگر جایزه در قالب پول نقد به محققان امنیتی پرداخت شود، این بستر 20 درصد از این پاداش را به‌عنوان سود برای خود برمی‌دارد.

پروژه‌ای واجد شرایط استفاده از این سرویس خواهد بود که دارای مجوز طرح متن‌باز بوده و حداقل برای 3 ماه فعال بوده باشد. پروژه‌های پذیرفته‌شده ملزم هستند یک پرونده با نام SECURITY.md را به ریشه‌ی پروژه‌ی خود اضافه کنند تا جزئیات ارسال آسیب‌پذیری، تبلیغات مربوط به برنامه در وب‌گاه پروژه و ارسال پاسخ به گزارش ارسال‌شده در عرض یک هفته، برای آن‌ها فراهم شود.

بستر HackerOne و Synack در مجموع 7 میلیون دلار پاداش دریافت کرده‌اند تا به وزارت دادگستری آمریکا و و بخش‌های مختلف آن در اجرای برنامه‌ی پاداش در ازای اشکال کمک کنند. یکی از طرح‌هایی که توسط HackerOne انجام شد، برنامه‌ی نفوذ به ارتش آمریکا بود که در این برنامه بیش از 100 آسیب‌پذیری ارسال شد و به شرکت‌کنندگان به‌طور میانگین 100 هزار دلار جایزه پرداخت شد.

اخبار فنی

آسیب‌پذیری موجود در آپاچی Struts، در دنیای واقعی مورد بهره‌برداری قرار می‌گیرد

محققان امنیتی سیسکو تالوس می‌گویند یک آسیب‌پذیری اجرای کد از راه دور با درجه‌ی اهمیت بالا که چارچوب آپاچی Struts 2 را تحت تأثیر قرار می‌دهد، در دنیای واقعی در حال بهره‌برداری است.

این آسیب‌پذیری با شناسه‌ی CVE-2017-5638 زمانی مورد بهره‌برداری قرار می‌گیرد که بارگذاری یک پرونده با استفاده از تجزیه‌کننده‌ی Jakarta Multipart اجرا می‌شود. این آسیب‌پذیری از استفاده‌ی نادرست از سرآیند نوع محتوا، ناشی می‌شود و به مهاجم غیرمجاز و راه دور اجازه می‌دهد بر روی سامانه‌ی هدف دستورات سامانه عامل را اجرا کنند.

این آسیب‌پذیری نسخه‌های 2.3.5 تا 2.3.31 و 2.5 تا 2.5.10 چارچوب Struts را تحت تأثیر قرار می‌دهد و چند روز پیش با انتشار نسخه‌های 2.3.32 و 2.5.10.1 وصله شده است. بلافاصله بعد از اینکه یک نفر کد اثبات مفهومی برای بهره‌برداری از این آسیب‌پذیری را منتشر کرد، محققان تالوس متوجه بهره‌برداری از آن در دنیای واقعی شدند. محققان می‌گویند اکثر این بهره‌برداری‌ها با استفاده از کد اثبات مفهومی انجام می‌شود.

در برخی از این حملات از دستورات معمول لینوکس استفاده می‌شود. مهاجمان با این کار می‌خواهند تشخیص دهند آیا دستگاه هدف دارای آسیب‌پذیری هست یا خیر. محققان می‌گویند شاهد استفاده از دستوراتی مانند whoami و ifconfig بوده‌اند تا سرویس‌هایی که کاربر مورد استفاده قرار می‌دهد را شناسایی و به اطلاعات پیکربندی شبکه‌ی قربانی دست یابند.

در برخی از حملات پیچیده، مهاجمان دیواره‌ی آتش سامانه‌ی هدف را مورد بررسی قرار داده و از روی کارگزار وب، بار داده‌ی مخرب بارگیری کرده و در ادامه آن را اجرا می‌کنند. محققان سیسکو می‌گویند این بار داده حاوی بات‌های IRC، منع سرویس و بدافزار بیل‌گیتس است.

در برخی دیگر از حملات، برای داشتن ماندگاری بر روی سامانه، مهاجمان بدافزار را در داخل پوشه‌های راه‌اندازی سامانه رونویسی می‌کنند. در این حملات همچنین در زمان راه‌اندازی سامانه، دیواره‌ی آتش غیرفعال می‌شود.

یکی از کارشناسان سیسکو می‌گوید: «احتمال دارد در ادامه شاهد بهره‌برداری گسترده از این آسیب‌پذیری باشیم چرا که بهره‌برداری از آن بسیار آسان بوده و تعداد زیادی دستگاه آسیب‌پذیر وجود دارد.»

محققان می‌گویند تعداد زیادی از وب‌گاه‌ها که دارای این آسیب‌پذیری بودند و آلوده شده‌اند درصدد رفع آلودگی برآمده‌اند. به کاربران توصیه شده است در اسرع وقت برنامه‌های آپاچی Struts را به‌روزرسانی کنند. شرکت Qualys نیز برای این آسیب‌پذیری یک مشاوره‌نامه منتشر کرده است.

اخبار فنی

کشف یک دربِ پشتی در تجهیزات اینترنت اشیاء متعلق به شرکت چینی DblTek

GoIP-8

محققان امنیتی یک دربِ پشتی در دستگاه‌های اینترنت اشیاء که توسط شرکت چینی DblTek تولید می‌شود، کشف کردند. این شرکت از برطرف کردن این اشکال امتناع می‌کند.

این شرکت در حوزه‌ی VoIP فعالیت دارد و محققان حدس می‌زنند این دربِ پشتی برای اهداف عیب‌یابی توسعه داده شده است. کارشناسان امنیتی کشف کردند واسط Telnet متعلق به GoIP دارای یک کاربر غیررسمی با نام dbladm است که دسترسی شِل با سطح ریشه را برای دستگاه فراهم می‌کند. این حساب با هیچ گذرواژه‌ای محافظت نمی‌شود و در عوض از یک سازوکار احراز هویت چالش-پاسخ بهره می‌برد.

وقتی مهاجم تلاش می‌کند بر روی دستگاه تحت عنوان کاربر dbladm، پروتکل Telnet را اجرا کند، مؤلفه‌های اینترنت اشیاء تلاش می‌کنند بر روی درگاه 11000 پروتکل UDP به آدرس 192.168.2.1 بر روی شبکه‌ی محلی متصل شوند. اگر دستگاه آسیب‌پذیر، پاسخ معتبری را دریافت کند، دسترسی‌ها به او اعطا خواهد شد.

محققان این اشکال را به شرکت تولیدکننده گزارش دادند ولی این شرکت تنها به انتشار یک ثابت‌افزار اکتفا کرد که در آن تغییرات بسیار کمی ایجاد شده و دسترسی به این سرویس همچنان باز است. این شرکت در ادامه نیز تماس خود را با محققان امنیتی قطع کرد. محققان کد بهره‌برداری از این دربِ پشتی را بر روی نسخه‌های قدیمی و جدید ثابت‌افزار این دستگاه‌ها توسعه داده بودند.

ثابت‌افزارهای آسیب‌پذیر در دستگاه‌های GSM به VoIP این شرکت وجود دارد و در شرکت‌های کوچک تا متوسط مورد استفاده قرار می‌گیرند. پویشی که برای پیدا کردن دستگاه‌های آسیب‌پذیر انجام شده، نشان می‌دهد صدها دستگاه در سطح اینترنت دارای این آسیب‌پذیری هستند.

اخبار فنی

با انتشار نسخه‌ی جدید وردپرس، ۶ آسیب‌پذیری وصله شد

روز دوشنبه توسعه‌دهندگان وردپرس انتشار نسخه‌ی 4.7.3 را اطلاع‌رسانی کردند. این نسخه‌ی جدید یک به‌روزرسانی امنیتی بوده و در آن 6 آسیب‌پذیری وصله شده است. در نسخه‌ی 4.7.3 وردپرس 3 آسیب‌پذیری XSS برطرف شده است که با استفاده از فراداده‌های پرونده‌های رسانه‌ای، آدرس‌های URL ویدئوها در یوتیوب و نام طبقه‌بندی‌ها قابل بهره‌برداری بودند.

در آخرین نسخه‌ی وردپرس همچنین یک آسیب‌پذیری مربوط به فریب سازوکار اعتبارسنجی تغییر مسیر آدرس‌های URL وصله شده است. آسیب‌پذیری دیگر می‌تواند باعث شود تا مدیر سامانه، با قابلیت حذف افزونه‌ها برخی پرونده‌های ناخواسته را حذف کند. یکی دیگر از آسیب‌پذیری‌ها، یک اشکال CSRF در تابع Press This است. بهره‌برداری از این آسیب‌پذیری منجر به استفاده‌ی بیش از حد از منابع کارگزارها شده و شرایط حمله‌ی منع سرویس را پیش خواهد آورد.

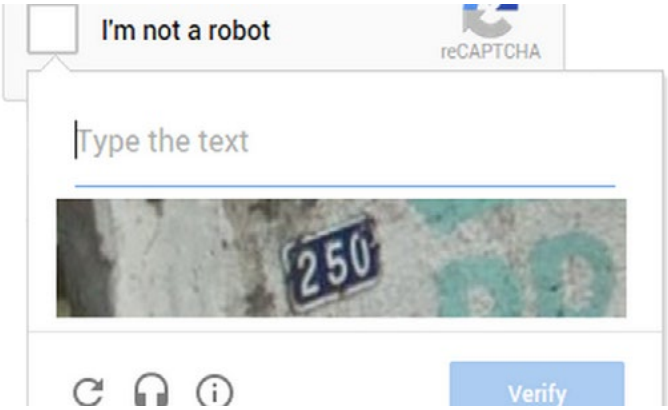
یک محقق امنیتی دیگر، دو آسیب‌پذیری XSS در قابلیت playlist وردپرس کشف کرده است. برای بهره‌برداری از این آسیب‌پذیری مهاجم نیاز دارد تا یک ویرایشگر یا مدیر وب‌گاه را به بارگذاری یک پرونده‌ی mp3 متقاعد کند. این پرونده حاوی فراداده‌های جعلی و ناقص است. کد مخربی که توسط مهاجم نوشته شده، زمانی اجرا می‌شود که این فراداده‌ها توسط توابع renderTracks() یا wp_playlist_shortcode() پردازش شوند.

در پروژه‌ی Summer of Pwnage بیش از 100 آسیب‌پذیری در هسته و افزونه‌های وردپرس کشف شده و همه‌ی آن‌ها خواه وصله شده یا نشده، در تاریخ 10 اسفند ماه افشاء شدند. یکی از آسیب‌پذیری‌های وردپرس در هسته‌ی آن که در سال 2016 کشف شده و هنوز هم وصله نشده، CSRF است. جزئیات این آسیب‌پذیری افشاء نشده ولی محققان امنیتی می‌گویند بهره‌برداری از این آسیب‌پذیری به‌طور تئوری، به مهاجم اجازه می‌دهد تا گواهی‌نامه‌های FTP و SSH را به سرقت ببرد. محققان می‌گویند این آسیب‌پذیری می‌تواند تأثیرات بسیار زیادی داشته باشد ولی احتمال بهره‌برداری از آن بسیار کم است.

هرچند توسعه‌دهندگان وردپرس اعلام کرده‌اند که در نسخه‌ی 4.7.3 شش مورد آسیب‌پذیری وصله شده ولی هنوز آسیب‌پذیری‌هایی هستند که وصله نشده‌اند و این شرکت برای حفاظت از کاربران خود، در حال حاضر آن‌ها را افشاء نکرده است. نسخه‌ی 4.7.2 در تاریخ 7 بهمن ماه منتشر شد و اعلام شده بود تنها 3 آسیب‌پذیری را وصله کرده است. در حالی‌که یک هفته بعد از آن دیدیم که دو آسیب‌پذیری حیاتی ارتقاء امتیاز و تزریق محتوا نیز در این نسخه وصله شده بود.

اخبار فنی

با استفاده از ابزارهای گوگل، سامانه‌ی ری‌کپچای این شرکت دور زده شد



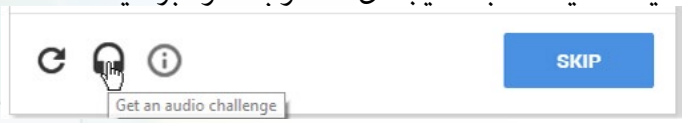
روز سه‌شنبه اثبات مفهومی برای دور زدن سامانه‌ی اعتبارسنجی ری‌کپچای گوگل به‌طور برخط منتشر شده است. این سامانه با استفاده از سرویس‌های مبتنی بر وب گوگل دور زده می‌شود.

به گزارش محقق امنیتی که این ابزار را توسعه داده، این ابزار با نام ReBreakCaptcha می‌تواند نسخه‌ی 2 ری‌کپچای گوگل را در هر جای وب دور بزند. گوگل سرویس ری‌کپچا را در سال 2014 معرفی کرد. این سامانه تلاش دارد از ایجاد صدها حساب کاربری به‌طور همزمان توسط بات‌ها و اسکریپت‌ها جلوگیری کند.

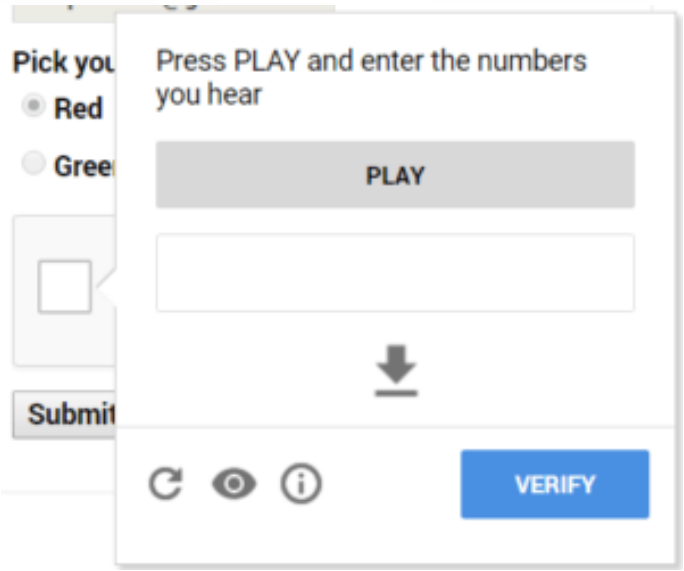
کپچا یک سرویس کاملاً خودکار است که تلاش دارد بین انسان و ماشین تمایز قائل شود. ری‌کپچا نامی است که گوگل برای سرویس و فناوری خود انتخاب کرده که در حال حاضر از متن، تصویر و صوت به‌عنوان چالش استفاده می‌کند تا مطمئن شود واقعاً یک انسان می‌خواهد وارد حساب کاربری شود.

شرکت گوگل دارای واسط برنامه‌نویسی است که کاربران با استفاده از آن می‌توانند چالش‌های کپچای صوتی را در قالب پرونده‌های صوتی ذخیره کنند. توسعه‌دهنده‌ی ابزار ReBreakCaptcha با استفاده از این واسط برنامه‌نویسی توانسته است نسخه‌ی 2 ری‌کپچا را بشکند. او در ادامه از روش‌های تبدیل گفتار به متن استفاده کرده و متن بدست آمده را در فیلد متنی ری‌کپچا وارد می‌کند.

در اولین قدم، این محقق باید بتواند به چالش صوتی دست یابد که این کار بسیار راحت است و با کلیک بر روی نشانگر هدفون که در زیر کپچا وجود دارد، می‌تواند به درخواست چالش صوتی دست یابد. این محقق می‌گوید: «شاید برخی از شما متوجه شده باشید که بعضی وقت‌ها بجای چالش صوتی، یک متن نمایش داده می‌شود. برای دور زدن این متن و بدست آوردن چالش صوتی، می‌توانید بر روی گزینه‌ی «بارگیری مجدد چالش» کلیک کنید تا به نتیجه‌ی مطلوب خود برسید.»



زمانی که چالش صوتی نمایش داده شد، سامانه‌ی ری‌کپچا به شما اجازه می‌دهد آن را اجرا کنید و یا بارگیری نمایید. توسعه‌دهنده‌ی این ابزار می‌نویسد: «بیایید این پرونده‌ی صوتی را بارگیری کرده و آن را برای واسط برنامه‌نویسی تشخیص گفتار گوگل ارسال کنید. لازم به‌ذکر است قبل از انجام این کار، باید فرمت پرونده‌ی صوتی را به wav تبدیل کنید چرا که این از ملزومات سرویس تشخیص گفتار گوگل است. چگونه می‌توان پرونده‌ی صوتی را به سرویس تشخیص گفتار گوگل ارسال کرد؟ با استفاده از واسط برنامه‌نویسیِ گوگل»

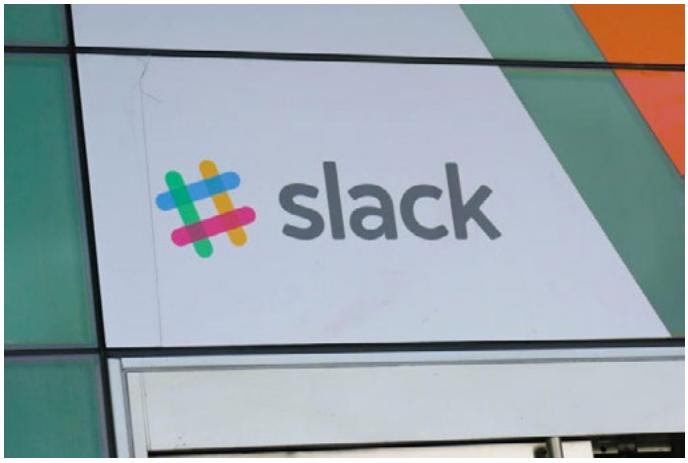


او در ادامه توضیح می‌دهد: «پس از ارسال پرونده‌ی wav به سرویس تشخیص گفتار گوگل، خروجی را در قالب متن دریافت خواهیم کرد. این خروجی، نتیجه‌ی مطلوب ما برای حل کردن چالش صوتی است.» بر روی گیت‌هاب، کد مفهومی این سامانه در قالب اسکریپت پایتون منتشر شده است.

این اولین بار نیست که سامانه‌ی ری‌کپچای گوگل دور زده می‌شود. سال گذشته در کنفرانس کلاه سیاه‌های آسیا، محققان از دانشگاه کلمبیا مقاله‌ای با عنوان «من انسان نیستم: دور زدن سامانه‌ی ری‌کپچای گوگل» منتشر کردند. در این مقاله برای دور زدن ری‌کپچا از تشخیص ویژگی‌ها و رفتارهای مشکوک مرورگرها استفاده شده بود. همچنین در این پژوهش از شناسایی و پیش‌بینی تصاویر در ری‌کپچا نیز استفاده شده بود. به‌گفته‌ی نویسندگان این مقاله، روش آن‌ها می‌تواند با دقت 70.78 درصد ری‌کپچاهای تصویری را حل کند و برای حل هر چالش تقریباً به 19 ثانیه زمان نیاز داشت.

اخبار فنی

آسیب‌پذیری در Slack و سرقت حساب‌های کاربری توسط مهاجمان



یک آسیب‌پذیری در کارخواهِ گفتگوی کاری Slack کشف شده که مهاجمان را قادر می‌سازد حساب‌های کاربری افراد را به سرقت برده و کنترل کاملی بر روی ارتباطات انجام‌شده در آن داشته باشند. خوشبختانه این آسیب‌پذیری وصله شده و شما می‌توانید برنامه‌های خود را به‌روزرسانی کنید.

این آسیب‌پذیری توسط یکی از محققان شرکت Detectify با نام فرانس روسن کشف شده است. به گزارش روسن، با وادار کردن کاربر برای بازدید از صفحات مخرب، مهاجمان می‌توانند رمزواره‌های Slack افراد را به سرقت ببرند.

روسن توضیح می‌دهد زمانی که می‌خواست با استفاده از مرورگرهای نسخه‌ی Slack تماس‌های سایر افراد را قطع کند، خودش با قطعی مواجه شده و متوجه شده مشکلی وجود دارد. یک آسیب‌پذیری دیگر که در بخش تماس‌ها وجود داشت به این محقق اجازه می‌داد تمامی پیام‌هایی که به برنامه‌های رایانامه‌ای ارسال می‌شد را شنود کند. روسن یک کد بهره‌برداری را توسعه داده که با استفاده از آن می‌توان از طریق صفحات وب مخرب، رمزواره‌های Slack را به سرقت برده و آن‌ها را ذخیره کرد. به‌طور خلاصه، زمانی‌که کاربر یک صفحه‌ی مخرب را باز می‌کند، تماس Slack باز می‌شود و یک WebSocket تلاش می‌کند او را به یک کارگزار مخرب متصل کند.

مهاجمان با بدست آوردن این رمزواره‌ها می‌توانند به حساب‌های کاربری افراد دست یابند و این موضوع بسیار نگران‌کننده است. Slack برای گزارش این آسیب‌پذیری 3 هزار دلار پاداش پرداخت کرد و در مدت چند ساعت آن را وصله نمود.

این محقق می‌گوید: «من تقریباً عصر روز جمعه، گزارش آسیب‌پذیری را برای Slack ارسال کردم. آن‌ها دقیقاً 33 دقیقه پس از گزارش اولیه به من پاسخ دادند و آسیب‌پذیری در عرض 5 ساعت وصله شد. این واقعاً شگفت‌انگیز است.»

اخبار فنی

شبیه‌ساز سرویس‌های آسیب‌پذیر برای متااسپلویت منتشر شد

ابزار جدیدی که می‌تواند سرویس‌های آسیب‌پذیر را شبیه‌سازی کرده و به استفاده‌ی بیشتر از بستر تست نفوذ متااسپلویت کمک کند، به‌طور متن‌باز منتشر شده است. متااسپلویت برای این طراحی شده تا محققان امنیتی بتوانند امنیت را از دیدگاه نفوذگران و مهاجمان ببینند ولی بدون داشتن سرویسی که دارای آسیب‌پذیری‌های مختلف باشد، رسیدن به این هدف سخت خواهد بود. تصاویر سامانه عاملِ آسیب‌پذیر، قبلاً در دسترس محققان قرار گرفته بود ولی این تصاویر کافی نبودند و تنها تعداد محدودی از ماژول‌های متااسپلویت در آن وجود داشت. شبیه‌ساز سرویس‌های آسیب‌پذیر، در گیت‌هاب منتشر شده و این مشکل را حل می‌کند. این شبیه‌ساز در قالب یک چارچوب طراحی شده و به محققان امنیتی اجازه می‌دهد به‌راحتی در محیط‌های آسیب‌پذیر، فعالیت‌های تست نفوذ انجام دهند.

توسعه‌دهنده‌ی این ابزار می‌گوید: «در حال حاضر، این سرویس بیش از 100 سرویس آسیب‌پذیر را شبیه‌سازی کرده و حملاتی همچون آلوده کردن گواهی‌نامه‌ها، گرفتن یک شِل از قربانی و غیره را پوشش می‌دهد. با استفاده از این ابزار، محققان می‌توانند با جزئیات آسیب‌پذیری‌ها آشنا شده و روش‌های مقابله با آن را یاد بگیرند.»

به گفته‌ی این محقق امنیتی، نصب و کار با این ابزار بسیار راحت بوده و تنها چیزی که نیاز دارد نصب پِرل بر روی ماشین‌های ویندوز، مک یا لینوکس است. همچنین این شبیه‌ساز طوری طراحی شده که مستقل از زبان است و سرویس‌ها را با قالب JSON شبیه‌سازی می‌کند. بنابراین هرکسی می‌تواند به‌راحتی، سرویسی را در JSON اضافه، ویرایش و یا حذف کند.

نکته‌ای که کاربران هنگام استفاده از این شبیه‌ساز باید به‌خاطر داشته باشند این است که هر دستوری که در شِل وارد می‌شود، در واقع بر روی سامانه‌ی هدف اجرا خواهد شد. برای همین این دستورات را در محیط‌های امن و مطمئن اجرا کنید تا مشکلی پیش نیاید.

شبیه‌ساز سرویس‌های آسیب‌پذیر، وسیله‌ای است که متخصصان حوزه‌ی فناوری اطلاعات و مهندسان می‌توانند از آن برای تست ماژول‌های متااسپلویت استفاده کرده و متااسپلویت را یاد بگیرند. نویسنده‌ی این ابزار گفته است: «در هسته‌ی این پروژه، چارچوبی را توسعه داده‌ایم که پرونده‌های توصیفی مبتنی بر JSON را اجرا می‌کند. پیاده‌سازی فعلی با استفاده از پِرل انجام شده اما شما می‌توانید بسته به اهداف خود، این چارچوب را با زبان برنامه‌نویسی دیگری پیاده‌سازی کنید.» جزئیات فنّی بیشتر در مورد این ابزار را می‌توانید در صفحه‌ی گیت‌هاب مشاهده کنید.

اخبار فنی

برای آسیب‌پذیری GDI ویندوز، وصله‌ی موقتی منتشر شد

دو هفته قبل یک آسیب‌پذیری در واسط دستگاه گرافیکی (GDI) ویندوز افشاء شد. اینک برای این آسیب‌پذیری یک وصله‌ی موقتی منتشر شده است. این آسیب‌پذیری اسفند ماه سال گذشته توسط یکی از مهندسان امنیتی گوگل در کنار سایر اشکالاتی که در کتابخانه‌ی GDI وجود داشت کشف شده بود. مایکروسافت تلاش داشت در به‌روزرسانی امنیتی خرداد ماه این آسیب‌پذیری را وصله کند ولی موفق نشد و سرانجام آبان ماه گزارشی در این خصوص منتشر کرد.

بنابر سیاست‌های افشای آسیب‌پذیری در گوگل، شرکت مربوطه 90 روز زمان دارد تا آسیب‌پذیریِ گزارش‌شده را وصله کند و پس از گذشت این مهلت، آسیب‌پذیری به‌طور عمومی افشاء خواهد شد. این موضوع در مورد آسیب‌پذیری در GDI نیز انجام شد. به‌دلیل اینکه مایکروسافت نتوانست به‌روزرسانی‌های امنیتی خود را برای ماه فوریه منتشر کند و آن را به ماه بعدی موکول کرد، این آسیب‌پذیری در طول بازه‌ی 90 روز وصله نشد. این آسیب‌پذیری با شناسه‌ی CVE-2017-0038 مربوط به نحوه‌ی پردازش بیت‌مپ‌های مستقل دستگاه (DIB) که در رکوردهای EMF تعبیه‌شده است. محقق امنیتی که این آسیب‌پذیری را کشف کرده می‌تواند از آن به‌طور محلی (در داخل برنامه‌ی اینترنت اکسپلورر) و از راه دور (در برنامه‌ی برخط آفیس و با پرونده‌ی docx حاوی رکورد مخرب EMF) بهره‌برداری کند.

هرچند تاکنون وصله‌ای برای این آسیب‌پذیری منتشر نشده ولی یکی از کارشناسان مایکروسافت پیشنهاد داده تا وصله‌ای موقتی برای آن ارائه شود. کارشناسان مایکروسافت با کد اثبات مفهومی که محقق شرکت گوگل منتشر کرده بود، کار کردند و فهمیدند زمانی‌که یک پرونده‌ی جعلی EMF در اینترنت اکسپلورر 11 بارگذاری می‌شود، این آسیب‌پذیری قابل مشاهده است.

با استفاده از این آسیب‌پذیری مهاجمان می‌توانند به داده‌های حساسی که برنامه در حافظه نگه می‌دارد دست یابند. همچنین می‌توان با بهره‌برداری از آن، حملاتی را انجام داد که نیاز به شکستن سازوکار حفاظتی ASLR دارند. این محقق امنیتی توضیح داد برای برطرف کردن این آسیب‌پذیری نیاز است تا اندازه‌ی بیت‌های بیت‌مپ مبدأ (cbBitsSrc) از حاصل‌ضرب طول و عرض مستطیل مبدأ در تعداد بایت‌هایی که برای نمایش یک پیکسل به کار می‌رود (cxSrc * cySrc * 4) کمتر باشد.

این وصله‌ی موقت برای آسیب‌پذیری GDI ویندوز بر روی ماشین‌هایی که عامل 0patch را نصب دارند، قابل دسترسی است. محقق امنیتی مایکروسافت می‌گوید این وصله‌ی موقتی برای سامانه عامل‌های ویندوز 10، 8.1 و 7 64 بیتی و ویندوز 7 32 بیتی ارائه شده است. همچنین باید اشاره کنیم محصولات امنیتی نیز برای کشف این آسیب‌پذیری به‌روزرسانی شده‌اند تا از حملات احتمالی جلوگیری کنند.

فصل پنجم

اخبار تحـــــلیلی

اخبار تحلیلی

آی‌بی‌ام: بهره‌برداری از آسیب‌پذیری Shellshock هنوز هم آسان و ارزان است

کارشناسان آی‌بی‌ام می‌گویند تقریباً دو و نیم سال از کشف آسیب‌پذیری Shellshock می‌گذرد و هنوز هم این تهدید مورد بهره‌برداری قرار می‌گیرد چرا که بهره‌برداری از آن بسیار آسان و ارزان است.

این آسیب‌پذیری شهریور ماه سال 93 کشف شد و در خط فرمان پیش‌فرض سامانه‌های لینوکس و یونیکس وجود دارد. یک مهاجم می‌تواند با بهره‌برداری از این آسیب‌پذیری دستورات با امتیازات بالا را از راه دور اجرا کند.

این آسیب‌پذیری با شناسه‌ی CVE-2014-6271 تعداد وسیعی از دستگاه‌ها مانند کارگزارهای وب، دستگاه‌های اینترنت اشیاء، چاپگرها، سامانه‌های سرگرمی خودکار، مسیریاب‌ها و سامانه‌های کارخانه‌ای را هدف قرار می‌دهد. سامانه‌های مک OS X نیز تحت تأثیر این آسیب‌پذیری قرار گرفته‌اند.

با توجه به اینکه بسیاری از برنامه‌های کاربردی برای اجرا شدن مبتنی بر خط فرمان بَش هستند، مهاجم می‌تواند مجموعه دستورالعمل‌ها را به سمت کارگزاهای وب ارسال کرده و از این آسیب‌پذیری بهره‌برداری کند.

پس از اینکه این آسیب‌پذیری به‌طور عمومی افشاء شد، چندین گزارش در خصوص بهره‌برداری از آن در دنیای واقعی منتشر شد.

در خرداد ماه سال 94 هشدار دادند که هنوز هم از آسیب‌پذیری Shellshock بهره‌برداری می‌شود و اینک شاهد هستیم این روند بهره‌برداری و حمله با گذشت بیش از دو سال، همچنان ادامه دارد. تا به امروز بسیاری از دستگاه‌ها این آسیب‌پذیری را وصله نکرده‌اند و برای همین مهاجمان می‌توانند آن‌ها را هدف قرار دهند.

کارشناسان آی‌بی‌ام توضیح داده‌اند: «مهاجمان برای انجام این حمله به یک کارگزار، مهارت برنامه‌نویسی و بدافزار مورد نظر برای اجرا نیاز دارند. سطح دانش و مهارت موردنیاز برای انجام این حمله بسیار پایین است. مهاجمان می‌توانند در هر دقیقه این حمله را علیه صدها آدرس IP در سطح اینترنت انجام داده و منتظر شانس خود باشند تا چند مورد از این سامانه‌های هدف دارای آسیب‌پذیری باشند.»

محققان امنیتی می‌گویند برای انجام این حمله یک مهاجم به 5 دلار هزینه در ماه نیاز دارد. با پرداخت 30 دلار مهاجم می‌تواند در بازه‌ی 6 ماه، یک میلیون کارگزار را هدف قرار دهد و تقریباً 10 درصد از این سامانه‌ها می‌توانند وصله‌نشده باشند.

برای انجام حمله، مهاجم به یک کارگزار وب نیاز دارد تا کد مخرب را بر روی آن قرار دهد حال این کارگزار می‌تواند آپاچی یا lighthttp باشد. محققان آی‌بی‌ام برای اینکه نشان دهند این حمله چقدر آسان است کدهای پایتون برای بهره‌برداری از این آسیب‌پذیری را منتشر کردند.

یـک اسـکریپت بَـش می‌توانـد از کارگـزار وب یـک بـات را بارگیـری کـرده و آن را در مسـیر مشـخصی ذخیـره کنـد. در ادامـه نیـز پرونـده را بـه حالـت اجرایـی در آورده و اجـرا کنـد. مهاجـم می‌توانـد بـا سـازوکارهای مانـدگاری، پـس از راه‌انـدازی مجـدد سـامانه، بـات را اجـرا کنـد. در ادامـه مهاجـم می‌توانـد از خـط فرمـان بَـش اسـتفاده کـرده و از آسـیب‌پذیری Shellshock بهره‌بـرداری کنـد.

محققـان می‌گوینـد: «بـا کمـی مهـارت برنامه‌نویسـی، مهاجـم می‌توانـد در یـک حلقـه یـک بـازه از سـامانه‌های شـبکه و یـا کل اینترنـت را هـدف قـرار دهـد.» در انتهـا بایـد گفـت داشـتن یـک کارگـزار وب بـرای بهره‌بـرداری از Shellshock بـه مـدت ماه‌هـا بـرای مهاجـم بسـیار ارزان و راحـت اسـت.

اخبار تحلیلی

چگونه داده‌های دیجیتال را در DNA ذخیره‌سازی کنیم؟

آیا می‌دانید یک گرم DNA می‌تواند 1 میلیارد ترابایت داده را برای بیش از هزار سال ذخیره کند؟ سال گذشته شرکت مایکروسافت 10 میلیون رشته DNA مصنوعی از مرکز زیست‌شناسی دانشگاه سان‌فرانسیسکو خریداری کرد و در حال حاضر با محققان این مرکز همکاری دارد تا از این رشته‌ها به‌عنوان رسانه‌ای برای ذخیره‌سازی داده‌ها استفاده کند.

در آخرین آزمایش، دو محقق از دانشگاه کلمبیا و مرکز ژن نیویورک با همکاری هم، ذخیره‌سازی داده‌ها در DNA را بررسی کردند و نتایج این آزمایش بسیار شگفت‌انگیز بود. آن‌ها توانستند در یک گرم DNA با موفقیت 214 پتابایت داده را ذخیره‌سازی کنند. تحقیقات جدید درباره‌ی این موضوع در مجلات علمی منتشر شده است.

محققان چگونه داده‌های دیجیتال را در DNA ذخیره می کنند ؟

در فرآیند ذخیره‌سازی، داده‌ها در یک پرونده‌ی آرشیوی یکپارچه فشرده می‌شود. در ادامه این پرونده به رشته‌های کوچکی از مقادیر بایتری (صفرها و یک‌ها) تقسیم می‌شود. با استفاده از الگوریتم اصلاح-پاک‌کننده، بسته‌ها به‌طور تصادفی در قطره‌هایی درج می‌شوند. هر قطره دارای بارکد است که با استفاده از آن، محققان می‌توانند پرونده‌ها را دوباره بازسازی کنند.

محققان در ادامه هریک از صفر و یک‌ها را به یکی از بازهای نوکلئوتیدی در DNA با نام‌های A، G، C و T نگاشت می‌کنند. این فرآیند در نهایت با فهرستی از 72 هزار رشته‌ی DNA که داده‌ها در آن کد شده است، پایان می‌یابد. این داده‌ها در قالب یک پرونده‌ی متنی به مرکز زیست‌شناسی ارسال شده و در داخل DNA های بیولوژیکی قرار می‌گیرد.

محققان امنیتی معتقدند DNA یک رسانه‌ی ذخیره‌سازی بسیار جمع‌وجور است و می‌تواند اگر در مکان خشک و خنک نگهداری شود، صدها هزار سال سالم باقی بماند. به‌عبارت دیگر، DNA متراکم‌ترین رسانه‌ی ذخیره‌سازی است که تاکنون مشاهده شده است.

دنیای دیجیتال بزرگ و بزرگ‌تر می‌شود و تخمین زده شده، تعداد بیت‌های دیجیتال در سال 2020 با تعداد کل ستارگان در جهان برابر خواهد شد و داده‌های دیجیتال به 44 زتابایت یا 44 تریلیون گیگابایت خواهد رسید. بنابراین DNA ها به سازمان‌های بزرگ این امکان را می‌دهند که حجم زیادی از داده‌ها بر روی آن‌ها ذخیره شده و صدها سال بتوان این داده‌ها را از روی آن خواند.

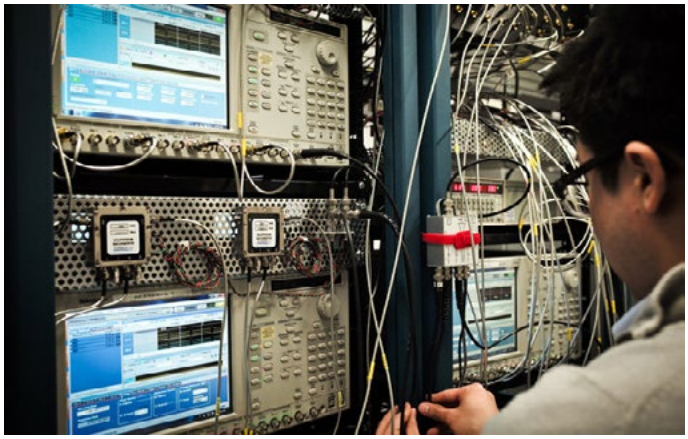
با این‌حال، هزینه‌ی استفاده از DNA نیز قابل توجه است. محققان برای ذخیره‌سازی 2 مگابایت داده 7 هزار دلار و برای خواندن آن 2هزار دلار هزینه کردند. با این‌حال، هنوز انتظار نداریم این فناوری به‌زودی به رسانه‌ای اصلی برای ذخیره‌سازی داده‌ها تبدیل شود. برای

مشـاهده‌ی جزئیـات بیشـتر در مـورد ایـن فنـاوری می‌توانیـد بـه ایـن پیونـد مراجعـه کـرده یـا ویدئـوی مربـوط بـه آن را مشـاهده کنیـد.

ASADAL INTERNET, INC. started its business in Seoul Korea in February 1998 with the fundamentalgoal of providing better internet services to the world. ASADAL stands for the "morning land" in ancient Korean. Asadal has about 35 staffs including well experienced web designers, programmers, and server engineers.

اخبار تحلیلی

برنامه‌ی Q شرکت آی‌بی‌ام شامل رایانه‌ی کوانتومی 50 کیوبیت است



در فیلم‌ها و سریال‌های تلویزیونی همیشه شاهد هستیم که شخصیت‌هایی با نام Q همیشه استثنایی هستند. در فیلم جیمز باند شخصیت Q در خدمت گجت‌ها بود. اینک آی‌بی‌ام نیز برنامه‌ی محاسبات کوانتومی با نام Q را تولید کرده که در نوع خود قابل توجه خواهد بود.

چندین سال است که شرکت آی‌بی‌ام تلاش دارد کامپیوتر کوانتومی با بیش از 50 کیوبیت را طراحی کند و رایانه‌های معمولی را مغلوب فناوری خود سازد. آی‌بی‌ام Q قرار است سرویس‌های محاسبات کوانتومی سریع را به کاربران ارائه کند. این سامانه قادر خواهد بود وظایفی را انجام دهد که رایانه‌های معمولی قادر به اجرای آن نیستند. آی‌بی‌ام اعلام کرد این سامانه اکتشافات علمی را سرعت خواهد بخشید.

رایانه‌های کوانتومی کاملاً با سامانه‌های معمولی متفاوت هستند و در آینده می‌توانند جایگزین رایانه‌ها و کارگزارهای فعلی شوند. با استفاده از رایانه‌های کوانتومی انجام محاسباتی که رایانه‌های معمولی در انجام آن محدود هستند، با سرعت بالایی انجام خواهد شد.

آی‌بی‌ام در حال ساخت رایانه‌های کوانتومی سریع است تا ثابت کند، ساخت چنین سامانه‌هایی یک رویای تئوری نیست. هدف نهایی آی‌بی‌ام این است که یک رایانه‌ی کوانتومی جهانی طراحی کند که دارای هزاران کیوبیت است و می‌تواند وظایف محاسباتی بسیار پیچیده را اجرا کند.

مدیر بخش محاسبات کوانتومی آی‌بی‌ام می‌گوید رایانه‌ی کوانتومی 50 کیوبیت برای حل الگوریتم‌ها و برخی مسائل دنیای واقعی، اندازه‌ای کافی و مناسب است. او گفت اگر بتوانیم رایانه‌های سریع را توسعه دهیم می‌توانیم کاربردهای جدیدی را پیدا کنیم که قبلاً انتظار آن را نداشتیم و رایانه‌های کوانتومی می‌توانند به این کاربردها کمک کنند.

رایانه‌های کوانتومی می‌توانند در حل مسائلی مانند کشف داروها، حل مسائل ساختارهای مولکولی که بودن زوایای مختلف یک شکل بسیار مشکل‌ساز است، کمک‌کننده باشند. حل این مسائل با استفاده از رایانه‌های کنونی بسیار سخت است چرا که منابع انرژی بسیار زیادی نیاز دارد.

به‌نظر می‌رسد تجاری‌سازی رایانه‌های کوانتومی توسط آی‌بی‌ام کمی زود باشد چرا که این رایانه‌ها هنوز در مرحله‌ی تحقیق و پژوهش قرار دارند. واکنش‌ها نسبت به رایانه‌ی کوانتومی 50 کیوبیت آی‌بی‌ام بسیار جالب بوده است. این رایانه از سال قبل با 40 هزار کاربر در حال اجرا شدن است و 200 هزار آزمایش بر روی آن انجام شده و محققان خارجی در مورد آن 15 مقاله‌ی تحقیقاتی منتشر کرده‌اند.

رایانه‌های کوانتومی کوچک آماده شده‌اند تا بر روی آن‌ها برنامه‌ی Q آی‌بی‌ام نصب و اجرا شود. رایانه‌های

کوانتومی بزرگ‌تر توسط آی‌بی‌ام طراحی خواهد شد و نیازمند سازوکارهایی برای تأمین توان و سامانه‌ی خنک‌کننده است. در حال حاضر رایانه‌ی کوانتومی آی‌بی‌ام در بستر اَبر عمومی قرار گرفته و با نام «تجربه‌ی کوانتومی» به‌طور رایگان در اختیار کاربران خواهد بود.

ساخت رایانه‌های کوانتومی چالش بزرگی محسوب می‌شد چرا که این سامانه‌ها به‌شدت ناپایدار هستند. رایانه‌های امروزی بیت‌ها را در قالب 0 و 1 ذخیره می‌کنند در حالی‌که کیوبیت‌ها می‌توانند وضعیت‌های مختلفی داشته باشند. به‌طور مثال همزمان مقدار 0 و 1 را باهم داشته باشند. این فناوری فراموقعیت نام دارد و به رایانه‌های کوانتومی این امکان را می‌دهد تا به قدرت پردازشی و محاسباتی بالاتری دست یابند.

نکته‌ای که باید در مورد کیوبیت‌ها ذکر کنیم این است که کیوبیت‌ها بسیار شکننده هستند و می‌توانند به‌راحتی در اثر تابش الکترومغناطیسی تحت تأثیر قرار بگیرند و در نتیجه چرخه‌ی محاسباتی بهم بخورد. رایانه‌های کوانتومی نیازمند تثبیت هستند تا در کاربردهای ویژه مانند تعیین توالی ژنوم‌ها به‌کار آیند. در چنین فرآیندی نیازمند این هستیم که محاسبات حداقل در طول یک دور پایدار و ثابت باقی بماند.

مسئولان آی‌بی‌ام اعلام کردند در حال حاضر بر روی مشکلاتی که در مورد کیوبیت‌ها وجود دارد، کار می‌کنند و تلاش دارند به‌زودی موفقیت رایانه‌ی کوانتومی خود را به اثبات برسانند. تمرکز اصلی رایانه‌های 50 کیوبیت کوانتومی بر روی تثبیت کیوبیت‌ها و تصحیح خطا خواهد بود.

علاوه بر آی‌بی‌ام شرکت‌های دیگری مانند اینتل و مایکروسافت نیز بر روی رایانه‌های کوانتومی تحقیق می‌کنند و این بررسی صرفاً به‌طور تئوری پیش می‌رود. شرکت D-Wave یک رایانه‌ی کوانتومی با نام فولاد کوانتومی 2000 کیوبیتی را با قیمت 15 میلیون دلار عرضه می‌کند که در نهایت بر روی بستر اَبر ارائه خواهد شد. شرکت آی‌بی‌ام اخیراً رایانه‌ای را مبتنی بر تراشه‌هایی که از مغز الهام گرفته‌شده و شبیه به پردازنده‌های آزمایشگاهی TrueNorth است توسعه داده است. این رایانه‌ها برای وظایفی مانند الگوریتم‌های یادگیری ماشین طراحی شده‌اند که امروزه به‌راحتی با استفاده از رایانه‌های معمولی نیز انجام می‌شوند.

آی‌بی‌ام همچنین کیت‌های توسعه‌ی نرم‌افزار و واسط‌های برنامه‌نویسی نیز عرضه می‌کند. بنابراین برنامه‌هایی که با واسط‌های برنامه‌نویسی معروف نوشته شده باشند می‌توانند در داخل رایانه‌های کوانتومی مورد استفاده قرار بگیرند.

ASADAL INTERNET, INC. started its business in Seoul Korea in February, 1998 with the fundamentalgoal of providing better internet services to the world. ASADAL stands for the "Mornlng land" in ancient Korean. Asadal has about 35 staffs including well experienced web designers, programmers, and server engineers.

اخبار تحلیلی

بدافزار پاورشِل، از پروتکل DNS به‌عنوان زیرساخت دستور و کنترل استفاده می‌کند

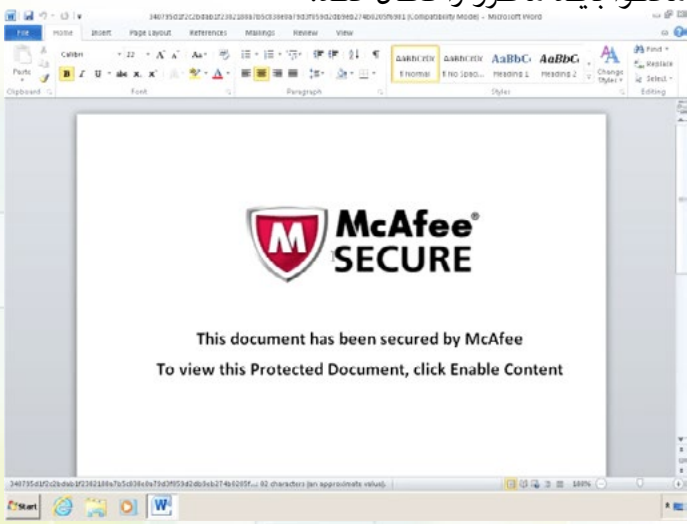
محققان سیسکو تالوس، بدافزاری را بررسی کردند که از اسکریپت پاورشِل برای واکشی دستورات از رکوردهای TXT سرویس DNS استفاده می‌کند.

کارشناسان تالوس گزارش مبسوطی را در مورد یک بدافزار ارائه کردند. این بدافزار در حملات هدفمند مورد استفاده قرار می‌گیرد و از اسناد مایکروسافت ورد استفاده می‌کند که از طریق هرزنامه توزیع می‌شوند.

کد مخربی که در این حملات مورد استفاده قرار می‌گیرد، مبتنی بر اسکریپت پاورشِل ویندوز است و ارتباط با زیرساخت دستور و کنترل با استفاده از سرویس نام دامنه (DNS) انجام می‌شود. مهاجمان از سرویس DNS برای ارتباط با کارگزار دستور و کنترل استفاده می‌کنند چرا که درخواست‌های DNS در شبکه‌های سازمانی هیچ‌گاه مسدود نمی‌شوند.

این کد مخرب اولین بار توسط محقق امنیتی با شناسه‌ی @simpo13 کشف شد. او در ادامه یافته‌ی خود را به محققان امنیتی سیسکو تالوس گزارش داد چرا که متوجه شد در این کد مخرب، ارجاعی به برنامه‌ی امنیتی SourceFire شرکت سیسکو وجود دارد. این ارجاع به شکل یک متن کدشده به‌صورت «SourceFireSux» است.

مهاجمان از یک روش مهندسی اجتماعی استفاده می‌کنند تا کاربران را وادار به باز کردن سند مخرب بکنند. در وبلاگ تالوس می‌خوانیم: «به‌طرز جالبی این سند ورد، طوری طراحی شده که به نظر می‌رسد از طریق سرویس رایانامه‌ی امن دریافت شده و با استفاده از مک‌آفی محافظت می‌شود. این روش احتمالاً به این خاطر استفاده شده که قربانی با مک‌آفی آشنا بوده و سریع به این سند اعتماد کرده و آن را باز می‌کند. این سند به کاربر اطلاعات می‌دهد که محافظت‌شده است و برای نمایش محتوا باید ماکرو را فعال کند.»



وقتی قربانی سند ورد را باز می‌کند، فرآیند آلودگی چندمرحله‌ای آغاز می‌شود. ابتدا با اجرا شدن یک پرونده‌ی ویژوال بیسیک یا ماکروی سند ورد، دستورات پاورشِل اجرا شده و یک دربِ پشتی بر روی ماشین نصب می‌شود. گروه تالوس در ادامه توضیح داد: «فهرست درهم‌سازی که در Pastebin وجود داشت ما را به سمت یک سند ورد هدایت کرد که بر روی یک جعبه

شنی عمومی بارگذاری شده بود. این سند نیز با فرآیند چندمرحله‌ای آلودگی آغاز شده بود و از طریق ماکروی مخرب فرآیند آلودگی را تکمیل می‌کرد.»

اسکریپت ویژوال بیسیک، یک پرونده‌ی فشرده و مبهم‌سازی‌شده‌ی پاورشِل را برای مرحله‌ی دوم، از بسته خارج می‌کند. این پاروشِل نسخه‌ی پاورشِلی که بر روی سامانه نصب شده را تشخیص می‌دهد و یک رکورد به رجیستری ویندوز اضافه می‌کند. در ادامه نیز یک پاورشِل را برای مرحله‌ی سوم آغاز می‌کند که به‌عنوان یک دربِ پشتی عمل می‌کند.

اگر کاربرِ قربانی دارای دسترسی‌های مدیریتی باشد، نصب‌کننده‌ی پاورشِل یک دربِ پشتی را در پایگاه داده‌ی ابزار مدیریت ویندوز (WMI) اضافه می‌کند تا پس از راه‌اندازی مجدد سامانه، دارای ویژگی ماندگاری باشد. زمانی‌که دربِ پشتی بر روی سامانه نصب شد، در مرحله‌ی چهارم حمله، کد مخرب به‌طور دوره‌ای درخواست‌های DNS را به سمت آدرس‌هایی که در اسکریپت هاردکد شده ارسال می‌کند.

رکوردهای TXT موجود در درخواست‌های DNS حاوی دستورات پاورشِل هستند که به‌طور مستقیم بر روی سامانه‌ی آلوده اجرا خواهند شد. نکته‌ی مهمی که وجود دارد این است که اطلاعات از رکوردهای DNS بازیابی شده ولی بر روی سامانه‌ی محلی نوشته نمی‌شود. اسکریپتی که در مرحله‌ی 4 مورد استفاده قرار می‌گیرد، در حقیقت ابزار کنترل از راه دور است که توسط مهاجمان بهره‌برداری می‌شود.

اگر دستوری از طرف مهاجمان از طریق رکوردهای DNS دریافت شود، بر روی سامانه اجرا شده و نتایج آن به سمت کارگزار دستور و کنترل ارسال می‌شود. این راه‌کار باعث می‌شود تا مهاجم قادر باشد هر دستور ویندوزی را بر روی سامانه‌ی قربانی اجرا کند.

محققان امنیتی نتوانستند زیرساخت ارتباطی و دستور و کنترل را مورد تحلیل و بررسی قرار دهند. این بدافزار نمونه‌ی عالی از حملاتی است که مهاجمان از پروتکلی استفاده کرده‌اند که فرآیند شناسایی را برای محققان سخت کرده است. از این به بعد باید در شبکه‌های سازمانی، پروتکل DNS را روشی بدانیم که مهاجمان از آن به‌عنوان زیرساخت دستور و کنترل استفاده می‌کنند.

ASADAL INTERNET, INC. started its business in Seoul Korea in February, 1998 with the fundamentalgoal of providing better internet services to the world. ASADAL stands for the "mythic land" in ancient Korean. Asadal has about 35 staffs including well experienced web designers, programmers, and server engineers.

اخبار تحلیلی

آسیب‌پذیری در توییتر به مهاجمان اجازه می‌دهد به حساب‌های قفل‌شده دست یابند

توییتر چند ماه قبل، تحت تأثیر یک آسیب‌پذیری قرار گرفته بود که مهاجمان با بهره‌برداری از آن می‌توانستند سازوکار قفل حساب‌های کاربری را دور بزنند. توییتر می‌تواند یک حساب کاربری را با اهداف امنیتی قفل کند. اگر توییتر رفتار مشکوکی را مشاهده کند که نشان دهد حساب کاربری در معرض خطر قرار گرفته، آن حساب را قفل می‌کند.

در این شرایط، کاربر برای اینکه حساب را از حالت قفل خارج کند، باید اثبات کند که مالک واقعی و قانونی این حساب است و اطلاعاتی از قبیل شماره‌ی تماس و آدرس رایانامه را ارائه دهد. یک محقق امنیتی با نام آرون اولگر، کشف کرد که این سازوکار قفل کردن حساب کاربری قابل دور زدن است. برای دور زدن این سازوکار کافی است مهاجم حساب مورد نظر را به دستگاه تلفن همراه اضافه کند.

این محقق حساب قفل‌شده را از طریق صفحه‌ی تنظیمات به دستگاه آیفون خود اضافه کرد. در ادامه نیز برنامه‌ی توییتر را بر روی تلفن همراه خود نصب کرده و به این حساب دسترسی کامل پیدا کرد. اولگر اشاره کرد هنوز هم بر روی وب‌گاه توییتر این حساب قفل‌شده باقی می‌ماند. برای دور زدن سازوکار بر روی برنامه‌ی تحت وب نیز مهاجم می‌توان در برنامه‌ی iOS به قسمت تنظیمات رفته و شماره تماس و آدرس رایانامه‌ی قربانی را بدست آورده و حساب را از حالت قفل خارج کند.

این آسیب‌پذیری می‌تواند برای مهاجمی که گواهی‌نامه‌های یک حساب را به‌سرقت برده و نمی‌خواهد حساب به‌خاطر رفتارهای مشکوک او قفل شود، مناسب باشد. این آسیب‌پذیری در تاریخ 16 مهر ماه به توییتر گزارش و چند روز بعد وصله شد. اولگر سال گذشته نیز گزارشی مبنی بر دور زدن سازوکار بازنشانی گذرواژه را در تامبلر منتشر کرده بود که با بهره‌برداری از آن می‌شد نقض داده‌ی بزرگی را انجام داد.

توییتر از سال 2014 میلادی بر روی بستر HackerOne برنامه‌ی پاداش در ازای اشکال برگزار کرده است. محققان با کشف آسیب‌پذیری اجرای کد از راه دور بر روی سرویس‌های اصلی توییتر می‌توانند مبلغ 15 هزار دلار جایزه دریافت کنند. به گزارش وب‌گاه HackerOne برای توییتر تاکنون 600 مورد آسیب‌پذیری گزارش شده است و این شرکت بیش از 600 هزار دلار پاداش به محققان امنیتی پرداخت کرده است.

اخبار تحلیلی

محققان می‌توانند با SGX اینتل بدافزارها را مخفی کرده و کلیدهای خصوصی را بدست آورند

گروهی از محققان امنیتی از دانشگاه صنعتی Graz اتریش تحقیقی را انجام داده و نشان دادند بدافزارهایی که بر روی اینتل SGX (افزونه‌ی گارد نرم‌افزاری) اجرا می‌شوند، می‌توانند برای سرقت کلیدهای رمزنگاری RSA مورد استفاده قرار بگیرند.

سازوکار SGX یک روش ایزوله‌سازی است که توسط اینتل در میکروپردازنده‌ها معرفی شده تا از تغییر و افشای داده‌ها و کد محافظت کند. این سازوکار از محیط اجرایی خاصی که به محیط‌های محصورشده مشهور هستند استفاده می‌کند و در ناحیه‌ی رمزنگاری‌شده‌ی حافظه کار می‌کند. بنابراین این سازوکار می‌تواند از اطلاعات محرمانه‌ی برنامه‌های کاربردی در برابر مهاجمان محافظت کند. اینتل می‌گوید کلیدهای رمزنگاری باید در این منطقه‌ی محصورشده نگهداری شوند چرا که مهاجمان با استفاده از حملات کانال-جانبی می‌توانند این کلیدها را به سرقت ببرند.

در حالی‌که برخی از محققان امنیتی بحث داشتند که ایزوله‌سازی مبتنی بر سخت‌افزار می‌تواند بدافزارها را به منطقه‌ی محصورشده راه بدهد ولی برخی دیگر این ترس‌ها را رد کرده و می‌گفتند منطقه‌ی محصورشده همواره با امتیازات فضای کاربری اجرا شده و نمی‌تواند عملیات I/O انجام دهد. در مقاله‌ی جدیدی که محققان دانشگاه صنعتی Graz منتشر کردند، ثابت شده بدافزارهای داخل منطقه‌ی محصورشده می‌تواند سامانه را هدف قرار دهد. در این مقاله می‌خوانیم: «ما وقوع یک حمله علیه حافظه‌ی نهان را نشان دادیم که با استفاده از یک بدافزار که در منطقه‌ی محصورشده قرار داشت انجام شده بود. در این منطقه کلیدهای رمزنگاری نیز قرار داشتند. بدافزار اثباتِ مفهومی ما می‌تواند کلیدهای رمزنگاری را از روی الگوی دسترسی به حافظه‌ی نهان بازیابی کند. این الگو حاصل از دسترسی فرآیند امضای RSA در یک حمله‌ی شبه-همگام به حافظه‌ی نهان است. کد بدافزار کاملاً از سامانه عامل مخفی است و نمی‌تواند مورد تجزیه و تحلیل قرار گیرد چرا که این کد در منطقه‌ی محصورشده قرار داشته و SGX از آن جلوگیری می‌کند.»

محققان می‌گویند در این حمله، بدافزار بر روی سخت‌افزار SGX در حال اجرا بوده و از ویژگی‌های آن بهره می‌برد. به‌عبارت دیگر بدافزار با استفاده از حفاظت‌های SGX می‌تواند خود را مخفی کند. نویسندگان مقاله عنوان کردند که قادر هستند این حمله را از روی سامانه‌ی بومی و همچنین از روی چندین کانتینر داکر انجام دهند. این حمله یک تهدید کانال-جانبی محسوب می‌شود.

باتوجه به عدم وجود تایمر، صفحات بزرگ، آدرس‌های فیزیکی و حافظه‌ی مشترک در محیط محصورشده‌ی SGX، این حمله موفقیت‌آمیز بوده است. علاوه بر این محققان می‌توانند در یک حمله‌ی شبه-همگام در 96 درصد از موارد، کلیدهای خصوصی RSA را بدست آورند.

در مقاله نشان داده شده است که هم برنامه‌ی هدف (که از SGX برای محافظت از کلیدهای RSA برنامه‌ها استفاده می‌کند) و هم کد مخرب دارای هیچ امتیازاتی نبوده و بر روی یک ماشین یکسان میزبانی می‌شوند. بدافزار، کد مخرب خود را در منطقه‌ی محصورشده‌ی SGX نگهداری می‌کند تا از فرآیند تشخیص جلوگیری شود. محققان می‌گویند اگر بر روی سامانه از روش‌های تشخیص بدافزار قدیمی استفاده شود، این بدافزار در محیط SGX هیچ‌گاه شناسایی نخواهد شد.

راه‌هایی برای مقابله با این‌گونه از حملات نیز ارائه شده است. توان بالا و برش بیت در سطح منبع، رنگ‌آمیزی محیط محصورشده، از بین بردن دسترسی به تایمرهایی با وضوح بالا، اجازه و دسترسی دادن به ارائه‌دهنده‌ی اَبر برای نظارت و پویش کد مخرب در محیط محصورشده، تصادفی کردن پشته، فناوری تخصیص حافظه‌ی نهان (CAT) در اینتل در سطح سامانه عامل، ترکیب فناوری CAT اینتل با SGX و استفاده از RAM امن در سطح سخت‌افزار از جمله روش‌های ارائه‌شده برای پیشگیری از این حملات است.

محققان امنیتی می‌گویند: «فناوری SGX با وجود محافظت‌هایی که با استفاده از مناطق محصورشده فراهم می‌کند، می‌تواند کدهای بدافزار را نیز مخفی کند. حتی با روش‌های پیشرفته‌ی تشخیص نیز نمی‌توان بدافزار ما را که در SGX قرار گرفته شناسایی کرد. اینتل بنابه دلایل امنیتی و عمداً فعالیت‌های SGX را در شمارنده‌ی کارایی قرار نمی‌دهد. با این‌حال، این سهل‌انگاری اینتل به مهاجمان اجازه می‌دهد تا بتوانند بدافزار خود را مخفی کنند.»

ASADAL INTERNET, INC. started its business in Seoul Korea in February, 1998 with the fundamentalgoal of providing better internet services to the world. ASADAL stands for the "Aromatic land" in ancient Korean. Asadal has about 35 staffs including well experienced web designers, programmers, and server engineers.

اخبار تحلیلی

در بدافزار شیمون ۲٫۰ ماژول باج‌افزاری کشف شد

محققان امنیتی آزمایشگاه کسپرسکی روز دوشنبه اعلام کردند، بدافزار شیمون 2.0 دارای یک ماژول باج‌افزاری کامل است و می‌تواند پرونده‌های موجود بر روی ماشین آلوده را رمزنگاری کند.

این شرکت امنیتی گزارشی فنّی از بدافزار شیمون 2.0 و قطعه‌ی بدافزاری جدید با نام StoneDrill را منتشر کرده است. کسپرسکی مدعی است این بدافزار جدید با گروه نفوذ ایرانی با نام Charming Kitten نیز مرتبط است.

ویژگی جالب توجهی که در بدافزار شیمون 2.0 کشف شده این است که علاوه بر اینکه می‌تواند بر روی سامانه‌ی هدف تمام پرونده‌های هارد دیسک را حذف کند، دارای یک ماژول باج‌افزاری کامل نیز هست. محققان امنیتی می‌گویند این ماژول باج‌افزاری در حال حاضر غیرفعال است ولی ممکن است در آینده و در حملات بعدی شیمون مورد استفاده قرار بگیرد.

زمانی که بدافزار شیمون، ماشینی را آلوده می‌کند، ابتدا زمان سامانه را مورد بررسی قرار می‌دهد تا بفهمد کی باید بار داده‌ی خود را نصب کند. پس از نصبِ بار داده، می‌تواند کل هارد دیسک را حذف کرده یا رمزنگاری کند.

کسپرسکی در گزارش خود می‌گوید: «در حالت باج‌افزار/رمزنگاری، یک کلید RC4 ضعیف و شبه‌تصادفی تولید می‌شود که در ادامه مستقیماً با کلید عمومی RSA رمزنگاری شده و در هارد دیسک ذخیره می‌شود. آفست این کلید در هارد دیسک 0x201 است و دقیقاً بعد از رکورد بوت اصلی قرار دارد.»

ماژول باج‌افزاری می‌تواند برای رمزنگاریِ مؤلفه‌های بدافزار شیمون و پرونده‌های ذخیره‌شده در پوشه‌های ویندوز مورد استفاده قرار بگیرد. بدافزار شیمون اولین بدافزار حذف‌کننده‌ی دیسک نیست که نویسندگان قابلیت باج‌افزاری به آن اضافه کرده‌اند. اواخر سال گذشته شاهد بودیم بدافزار KillDisk که در حملاتی علیه بخش‌های انرژی کشور اوکراین مورد استفاده قرار گرفته بود، تصمیم گرفت به‌جای حذف پرونده‌ها، آن‌ها را رمزنگاری کرده و از قربانیان باج درخواست کند.

تحقیقات کسپرسکی نشان می‌دهد منابعی که توسط بدافزار شیمون مورد استفاده قرار گرفته دارای شناسه‌ی زبان عربی یمنی هستند. شاید این نشانه‌ای باشد مبنی بر اینکه نویسندگان بدافزار شیمون یمنی هستند و عربستان سعودی را هدف قرار داده‌اند ولی این احتمال نیز وجود دارد که این یک نشانه‌ی گمراه‌کننده باشد. محققان امنیتی قبلاً این بدافزار را به کشور ایران نسبت داده بودند.

اخبار تحلیلی

حملات بر روی پروتکل DNS: چگونه به سمت وب‌گاه‌های جعلی هدایت می‌شویم؟

همه‌ی ما از اهمیت سرویس نام دامنه (DNS) مطلع هستیم و می‌دانیم برای عملکرد طبیعی اینترنت، این سرویس ضروری است و اگر DNS نبود شاید نمی‌توانستیم از اینترنت استفاده کنیم. با این‌حال بسیاری از کاربران خیلی متوجه اهمیت این سرویس نیستند و به آن توجه ندارند. تا زمانی‌که با استفاده از این پروتکل حمله‌ای رخ ندهد و اتفاق بدی پیش نیاید شاید متوجه نشویم که DNS چه نقش حیاتی را در اینترنت بازی می‌کند. به‌عنوان مثال در حمله‌ای که اخیراً باتنت Mirai علیه ارائه‌دهنده‌ی سرویس DNS با نام Dyn انجام داد، شاهد بودیم که بخش وسیعی از اینترنت با قطعی مواجه شد. نکته‌ای که باید اشاره کنیم، این است که حملات زیادی وجود دارد که می‌تواند این سرویس را تحت تأثیر قرار داده و از کار بیندازد. در این پست قصد داریم به انواع حملات بر روی پروتکل DNS بپردازیم و تفاوت بین آن‌ها را توضیح دهیم.

کارگزار DNS چیست؟

سرویس DNS پروتکلی است که ما را قادر می‌سازد آدرس URL یک صفحه‌ی وب را به آدرس IP آن تبدیل کنیم. با استفاده از این سرویس، دیگر لازم نیست برای هر صفحه‌ی وب، آدرس IP آن را به‌خاطر بسپاریم هرچند که این کار واقعاً سخت و غیرممکن است. تبدیل آدرس‌های دامنه به آدرس IP کاری است که کارگزارهای DNS انجام می‌دهند و برای این منظور به یک پایگاه داده‌ی توزیع‌شده و سلسله‌مراتبی مراجعه می‌کنند. در این پایگاه داده مشخص شده است هر آدرس URL مربوط به چه آدرس IP است. با این روش استفاده از آدرس‌های دامنه بسیار راحت‌تر شده و به‌عبارتی تغییر آدرس‌های IP متعلق به یک وب‌گاه نیز ممکن خواهد شد.

باتوجه به اهمیت سرویس DNS، خیلی عجیب نیست که شاهد حملاتی باشیم که از آسیب‌پذیری‌های موجود در این سرویس یا شیوه‌ای که کاربران از آن استفاده می‌کنند، بهره‌برداری کنند.

جعل DNS در مقابل مسمومیت حافظه‌ی نهان DNS

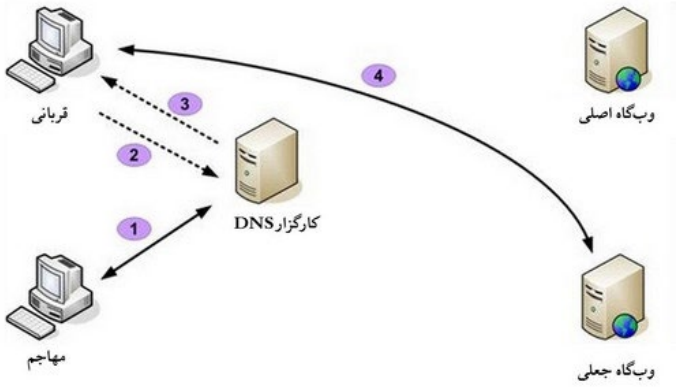
معمولاً این دو حمله با یک عنوان شناخته می‌شوند ولی در حقیقت این دو حمله از هم متفاوت هستند و به‌شیوه‌ای مختلف عمل می‌کنند. در حالت کلی می‌توان گفت، حمله‌ی مسمومیت حافظه‌ی نهان DNS یکی از چندین روشی است که می‌توان به جعل DNS رسید. در واقع این حمله، به گستره‌ی وسیعی از حملات اشاره دارد که تلاش می‌کنند آنچه در کارگزار DNS ذخیره شده را تغییر دهند.

هدف نهایی در حمله بر روی DNS می‌تواند این باشد که رکوردهای DNS بر روی کارگزار، به چیزی که مهاجم می‌خواهد، تغییر یابد که برای رسیدن به این هدف

روش‌های مختلفی وجود دارد. از جمله‌ی روش‌هایی که می‌توان رکوردهای DNS را جعل کرد، می‌توان مسمومیت حافظه‌ی نهان DNS، حمله‌ی مردِ میانی، استفاده از ایستگاه‌های پایه‌ی جعلی و تهدید کارگزار DNS را نام برد.

می‌توانیم مثال‌هی مختلفی از حمله‌ی جعل DNS را مشاهده کنیم. به‌طور مثال، مهاجمان می‌توانند آدرس کارگزار DNS که بر روی سامانه عامل یا مسیریاب شما پیکربندی شده را با آدرس دیگری جایگزین کنند. در حالت معمول باید آدرس کارگزار DNS را برابر با آدرس ارائه‌دهنده‌ی سرویس اینترنت خود یا سازمان دیگری مانند گوگل قرار دهیم.

حمله‌ی مسمومیت حافظه‌ی نهان DNS به شرایطی اشاره می‌کنند که همه یا تعداد زیادی از کاربران از یک حافظه‌ی نهان یکسان استفاده می‌کنند و هر آدرس IP به یک نام دامنه وابسته بوده و در قالب رکوردهایی ذخیره شده است. در این حمله، مهاجمان رکوردهای DNS را دست‌کاری کرده و ارائه‌دهندگان سرویس نیز این دست‌کاری را معتبر شناسایی کرده و قبول می‌کنند حتی اگر رکورد دست‌کاری‌شده به یک وب‌گاه جعلی اشاره کند.



در این شرایط، چیزی که ما شاهد هستیم این است که ترافیک ما به سمت آدرس IP قانونی هدایت نمی‌شود. هرچند انجام این مسمومیت در DNS به‌راحتی مسمومیت حافظه‌ی نهان در سامانه یا مسیریاب نیست ولی شواهد نشان می‌دهد این نوع از حملات شدنی است و نمونه‌هایی از انجام آن وجود دارد.

یکی از مشکلات اساسی که در حملات مسمومیت حافظه‌ی نهان DNS پیش می‌آید این است که این حمله می‌تواند به حافظه‌های نهان دیگر نیز گسترش پیدا کرده و ابعاد حمله را بزرگ‌تر کنند. به‌عنوان مثال فرض کنید حافظه‌ی نهان DNS بر روی سامانه‌ی شما آلوده شده است. رکوردهای دست‌کاری‌شده به سمت حافظه‌ی نهان DNS در مسیریاب نیز سرازیر شده و این حافظه با رکوردهای نادرست به‌روزرسانی خواهد شد.

حمله‌ی دامنه‌ربایی چیست؟

بدافزارها می‌توانند فرآیند ترجمه‌ی نام دامنه را نیز تحت تأثیر قرار دهند و قربانی به کارگزاری متصل شود که تحت کنترل مهاجمان است. به‌عنوان مثال می‌توان بدافزار Win32/DNSChanger را نام برد که می‌تواند درخواست‌های DNS را به سمت کارگزار جعلی تغییر مسیر دهد.

این حمله مهاجمان را قادر می‌سازد تا حملات بیشتری مانند فیشینگ را انجام دهد. در حملات فیشینگ، کاربر به سمت یک وب‌گاه جعلی هدایت شده و ممکن است گواهی‌نامه‌های خود را وارد کرده و این اطلاعات توسط مهاجمان به سرقت برود. در وب‌گاه‌های فیشینگ امکان توزیع بدافزار و بهره‌برداری از آسیب‌پذیری‌های موجود بر روی سامانه‌ی قربانی نیز وجود دارد.

همان‌طور که مشاهده کردید روش‌های مختلفی برای انجام حمله بر روی سرویس DNS وجود دارد و برای پیشگیری از چنین حملاتی لازم است که راه‌کارهای امنیتی مناسب بر روی سامانه‌ها نصب شده و بر فعالیت‌های صورت‌گرفته بر روی مسیریاب شبکه‌ها نظارت شود. به‌طور مداوم بررسی کنید تا مسیریاب شما به‌روز بوده و پیکربندی مناسبی داشته باشد. همچنین بر روی مسیریاب‌ها از گذرواژه‌های قوی استفاده کنید تا مهاجمان از راه دور نتوانند به آن نفوذ کنند.

اخبار تحلیلی

در توزیع باج‌افزار، حملات RDP نسبت به هرزنامه‌ها پیشی گرفته‌اند

پروتکل رومیزی راه دور (RDP) به‌طور چشمگیری به‌عنوان بردار حمله برای توزیع باج‌افزار مورد استفاده قرار می‌گیرد. این روش توزیع از چنان محبوبیتی برخوردار شده که از توزیع با ارسال هرزنامه نیز پیشی گرفته است. چندین سال است که از حملات RDP برای توزیع بدافزار استفاده می‌شود ولی اخیراً برای توزیع باج‌افزار مورد استفاده قرار گرفته‌اند. سال گذشته تعداد زیادی حمله‌ی جستجوی فراگیر بر روی گواهی‌نامه‌های RDP انجام دادند تا باج‌افزارها را توزیع کنند.

بررسی‌های شرکت ترندمیکرو در سال 2017 میلادی نشان داد که باج‌افزار Crysis در حال حاضر با استفاده از حملات RDP نیز انجام می‌شود. هرچند این نوع از حملات برای توزیع باج‌افزار از سال 2016 مشاهده شده ولی در ماه‌های اخیر، تعداد حملات RDP دو برابر شده است.

نموداری که اخیراً توسط شرکت‌های امنیتی منتشر شده نشان می‌دهد که توزیع باج‌افزار با استفاده از حملات RDP از توزیع با روش هرزنامه پیشی گرفته است. سهم حملات RDP برابر با 66 درصد و سهم هرزنامه 33 درصد بوده است. اگر بخواهیم از لحاظ تاریخی نیز به این موضوع توجه کنیم، باج‌افزارها با استفاده از روش‌های دیگری مانند کیت‌های بهره‌برداری و تبلیغ‌افزارها نیز توزیع می‌شوند ولی ترافیک مربوط به این بردارهای حمله قابل توجه نبوده و محبوبیتی بدست نیاورده است.

محققان امنیتی می‌گویند: «مشاهدات ما در دو ماه اخیر نشان می‌دهد که چقدر توجه به امنیت سرویس‌های RDP مهم است. سرویس‌های RDP ناامن می‌توانند دری برای نفوذ مهاجمان سایبری باشند. مهاجمان پیشرفته می‌توانند داده‌ها را بر روی سامانه‌ی هدف رمزنگاری کنند و آن‌ها را به سرقت نبرند و این مسئله‌ای است که کشف اینکه آن‌ها دقیقاً چه می‌خواهند را مشکل می‌کند.»

در بین باج‌افزارهای معروف Crysis مهم‌ترین بدافزاری است که با استفاده از حملات RDP توزیع می‌شود. در حال حاضر این باج‌افزار پسوند .wallet را به انتهای پرونده‌های رمزنگاری‌شده اضافه می‌کند و نسخه‌های مختلفی از این بدافزار تاکنون مشاهده شده است.

Expert Bulletin News

Information Communication Technology

2th year 2016 | Weekly bulletin

اخبار فناوری اطلاعات و ارتباطات

هفته نامه | شماره هشتاد و دوم | سال دوم | ۷۰ صفحه

خبرنامه هفتگی کارشناسی

مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج