سراج

۲۲ آبان ۱۳۹۵

شماره ۸۶

خبرنامه کارشناسی
اخبار فناوری اطلاعات و ارتباطات

مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج

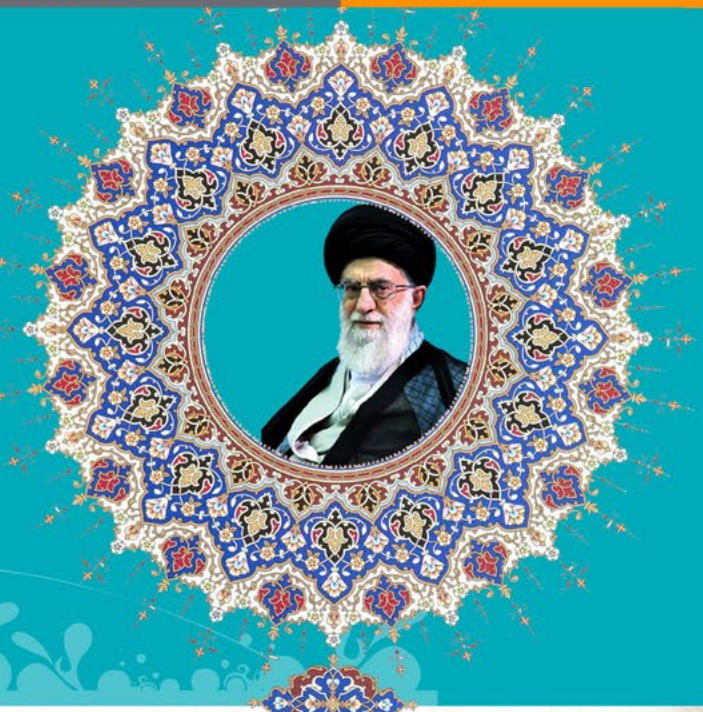
هفته نامه | شماره هشتاد و ششم | سال دوم | ۶۶ صفحه

Expert Bulletin News
Information Communication Technology
2th year 2016 | Weekly bulletin

در این شماره می‌خوانید:

بسم الله الرحمن الرحیم

آگاهی و بصیرت



جوان دانشجوی ما، افسر جوان است، شما که استاد او هستید، رتبهٔ بالاتر افسر جوانید. شما فرمانده ای هستید که باید مسائل کلان را ببینید.

مقام معظم رهبری (مد ظله العالی)

فهرست مطالب

فصل اول: اخبار عمومی

فصل دوم: مدیریت امنیت

فصل سوم: سیاست سایبری

فصل چهارم: اخبار فنی

فهرست مطالب

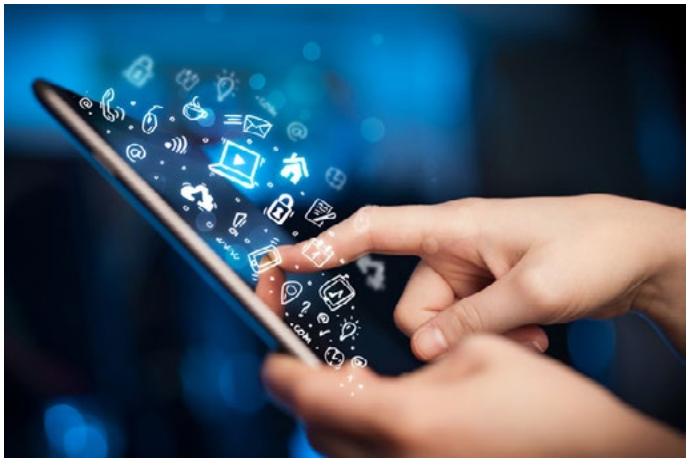
فصل پنجم: اخبار تحلیلی

فصل اول

اخبار عمومی

اخبار عمومی

امکان نفوذ به بیش از یک میلیارد برنامه‌ی تلفن همراه



محققان امنیتی توانسته‌اند راهی را برای هدف حمله قرار دادن برنامه‌های کاربردی اندرویدی و iOS پیدا کنند، راهی که به آن‌ها اجازه می‌دهد از راه دور و بدون اطلاع کاربر، وارد برنامه‌ی تلفن همراه وی شوند.

گروهی از محققان دانشگاه چینی هنگ‌کنگ دریافته‌اند که بیشتر برنامه‌های محبوب تلفن همراه که از سرویس تک‌مرحله‌ای (SSO) ورود به سامانه استفاده می‌کنند، به‌طور کاملاً ناامن OAuth 2.0 را در خود تعبیه کرده‌اند.

حتماً می‌دانید که OAuth 2.0 یک استاندارد باز برای احراز هویت است که به کاربران اجازه می‌دهد با تأیید هویت کنونی خود در شبکه‌های فیس‌بوک، گوگل یا حساب‌های کاربری شرکت چینی سینا، وارد سایر سرویس‌های شخص ثالث شوند.

این فرآیند کاربران را قادر می‌سازد که بدون نیاز به ارائه‌ی شناسه و گذرواژه وارد هر سرویس دیگری شوند.

توسعه‌دهندگان برنامه‌های کاربردی چگونه OAuth را تعبیه می‌کنند؟ (روش درست)

هنگامی‌که کاربر به وسیله‌ی OAuth وارد یک برنامه‌ی شخص ثالث می‌شود، این برنامه به کمک ارائه‌دهنده‌ی آن ID، مثلاً فیس‌بوک، بررسی می‌کند که آیا جزئیات مربوط به احراز هویت صحیح است یا خیر. اگر صحیح بود، OAuth یک «توکن دسترسی» را از فیس‌بوک دریافت می‌کند که در ادامه به کارگزار آن برنامه‌ی کاربردی تلفن همراه ارسال می‌شود.

هنگامی که توکن دسترسی صادر شد، کارگزار این برنامه اطلاعات احراز هویت کاربر را از فیس‌بوک درخواست می‌کند، آن‌ها را تأیید کرده، و سپس به کاربر اجازه می‌دهد با اطلاعات محرمانه‌ی فیس‌بوک وارد سامانه شود.

توسعه‌دهندگان برنامه‌های کاربردی چگونه OAuth را تعبیه می‌کنند؟ (روش نادرست)

پژوهش‌گران دریافته‌اند که توسعه‌دهنده‌ی تعداد بی‌شماری از برنامه‌های اندرویدی به درستی اعتبار اطلاعات ارسالی از سوی ارائه‌دهنده‌ی ID اعم از فیس‌بوک، گوگل یا سینا را بررسی نمی‌کنند.

ممکن است کارگزار این برنامه به جای تأیید اطلاعات OAuth (یعنی توکن دسترسی) مربوط به اطلاعات احراز هویت کاربر برای تأیید این‌که کاربر و ارائه‌دهنده‌ی ID به هم ربطی دارند یا خیر، فقط بازیابی ID کاربر از ارائه‌دهنده‌ی ID مربوطه را بررسی کند. به خاطر همین اشتباه، نفوذگران دارای دسترسی از راه دور می‌توانند این برنامه‌ی آسیب‌پذیر را بارگیری کنند، با اطلاعات شخصی خود به آن وارد شوند، سپس نام کاربری خود را به نام افرادی تغییر دهند که قصد حمله به آن‌ها را دارند، برای این کار می‌بایست کارگزار را به نحوی تنظیم کنند که

اطلاعات ارسالی از فیس‌بوک، گوگل یا هر ارائه‌دهنده‌ی ID دیگری را دست کاری نماید.

هر وقت این کار انجام شد، نفوذگران کنترل کامل داده‌های آن برنامه را در دست می‌گیرند.

دوست دارید نتیجه‌ی این ماجرا را بدانید؟ اگر نفوذگران وارد برنامه‌ی سفر کاربر قربانی شوند، می‌توانند از جدول برنامه‌های وی مطلع شوند؛ اگر آن‌ها وارد برنامه‌ی رزرو هتل شوند، می‌توانند اتاقی را برای خود رزرو کرد و پرداخت هزینه را به قربانی محول کنند؛ به بیان ساده نفوذگران می‌توانند داده‌های شخصی قربانی اعم از آدرس محل سکونت یا اطلاعات بانکی‌اش را بربایند.

محققا صدها برنامه‌ی محبوب اندرویدی چینی و آمریکایی را پیدا کرده‌اند که از سرویس SSO پشتیبانی می‌کنند، برنامه‌هایی که مجموع بارگیری‌های آن‌ها به ۲,۴ میلیارد می‌رسد و نسبت به این موضوع آسیب‌پذیر هستند.

با توجه به تعداد کاربرانی که از ورود مبتنی بر OAuth استفاده می‌کنند، محققان تخمین زده‌اند که بیش از یک میلیارد برنامه‌ی مختلف تلفن همراه در خطر نفوذ قرار داشته باشند.

پژوهش‌گران کدهای نفوذی خود را روی آیفون امتحان نکرده‌اند، اما بر این باورند که حملات آن‌ها روی هر برنامه‌ی آسیب‌پذیری در سامانه‌ی عامل iOS قابل اجرا خواهد بود.

اخبار عمومی

Privatoria: حفاظت از حریم خصوصی برخط شما به کمک یک سرویس VPN رمزشده

امروزه اکثر شما کاربران در شرایطی به گشت و گذار در اینترنت می‌پردازید که از این واقعیت خبر ندارید که وب‌گاه‌ها داده‌های شما را جمع‌آوری می‌کنند و موقعیت مکانی‌تان را ردیابی می‌کنند، و با اشتراک گذاشتن تاریخچه‌ی جست‌وجو، اطلاعات مکانی و نیز عادات خرید شما با تبلیغ‌کنندگان و بازاریابان، پول هنگفتی به چنگ می‌آورند.

اگر همه‌ی موارد فوق کافی نیست، بد نیست بدانید که نفوذگران و مجرمان سایبری وجود دارند که قادرند به راحتی داده‌های حساس و شخصی شما را از وب‌گاه‌های دارای تجهیزات اندک بربایند.

حقیقت تلخ‌تر این است که شما حریم خصوصی ناچیز و در حد صفری را در محیط‌های برخط تجربه می‌کنید. برای حل این مسئله، شما به یک شبکه‌ی خصوصی مجازی نیاز دارید؛ اگر تاکنون به اهمیت حریم خصوصی و استفاده از یک VPN فکر نکرده‌اید، شاید زمان آن فرا رسیده که تغییر رویه داده و اندکی بدان بیاندیشید.

متأسفانه همه‌ی VPNها به همان اندازه که ادعا می‌کنند ناشناس نیستند. برخی از این سرویس‌ها گزارش‌های گسترده‌ای را در رابطه با فعالیت کاربران خود در گستره‌ی وب نگهداری می‌کنند؛ مثلاً ممکن است آدرس‌های IP را هفته‌های متمادی ذخیره کنند و به این ترتیب فلسفه‌ی استفاده از یک شبکه‌ی مجازی خصوصی را زیر سؤال ببرند.

Privatoria یکی از VPNهایی است که نه‌تنها حفاظت در زمینه‌ی گشت و گذار در وب و نیز رمزگذاری ترافیک وب را ارائه می‌کند، بلکه گزارش‌های فعالیت‌های برخط شما را نیز به ثبت نمی‌رساند. Privatoria یک شرکت مستقر در جمهوری چک است که کار آن فراتر از ارائه‌ی راه‌کارهای VPN است. Privatoria علاوه بر «سیاست مخالفت با تهیه‌ی گزارش» شماری از قابلیت‌های مهم را در خود گنجانده که باعث می‌شود به یکی از بهترین سرویس‌های VPN موجود در بازار تبدیل شود.

این شرکت ارائه‌دهنده‌ی خدمات پیشرفته‌ای نظیر شبکه‌ی خصوصی مجازی یا همان وی‌پی‌ان، وی‌پی‌ان تور، پروکسی، پروکسی تور، و رایانامه‌های ناشناس است. حال قصد داریم نگاهی اجمالی به این قابلیت‌ها، مزایای آن‌ها و حوزه‌های استفاده‌شان بیاندازیم.

قابلیت‌های شبکه‌ی خصوصی مجازی Privatoria

1. مرور وب به‌صورت ناشناس

سامانه‌ی پنهان‌کننده‌ی IP این سرویس مانع آن می‌شود که سرویس‌های ارتباطی بتوانند موقعیت مکانی و جغرافیایی شما، آدرس IP یا نسخه‌ی مرورگرتان را برملا کنند.

2. ترافیکی که دو بار رمزگذاری شده است (VPN+TOR)

برای امنیت بیشتر می‌توانید Proxy Tor استفاده کنید که

هـر دو کانـال را به‌طـور هم‌زمـان بـه کار می‌گیـرد. بـه ایـن ترتیـب می‌توانیـد آدرس IP خـود را بـدون نیـاز بـه بارگیـری یـا نصـب هرگونـه نرم‌افـزار اضافـه‌ی دیگـری از تیـررس نـگاه نفوذگـران حفـظ کنیـد.

3. سیاست ضد تهیه‌ی گزارش

شـعار «ضـد داده‌کاوی» Privatoria را می‌توانیـد در هـر سرویـس دیگـری هـم ببینیـد. وی‌پـی‌ان Privatoria تضمیـن می‌کنـد کـه هیـچ گزارشـی از ترافیک‌هـا تهیـه نشـود، هیـچ در پشـتی تعبیـه نگـردد، و هیـچ مخزنـی از اطلاعـات کاربـران بـرای اشـخاص ثالـث ایجـاد نشـود.

4. ارسال رایانامه‌های امن

ایـن وی‌پـی‌ان بـه شـما ایـن فرصـت را می‌دهـد کـه از رمزگـذاری PGP رایانامـه بـا رمزنـگاری AES ۲۵۶ بیتـی نهایـت اسـتفاده را ببریـد.

5. کارگزار جهانی و سرعت شبکه

ایـن وی‌پـی‌ان قابلیـت اتصـال بـه ۶۳ کارگـزار تـور و نیـز ۱۹ کارگـزار پروکسـی/وی‌پی‌ان را در آمریـکا، انگلسـتان، کانـادا، فرانسـه، اسـپانیا، آلمـان، اسـترالیا، مـصر، سـنگاپور، و سـایر کشـورها دارد.

6. پشتیبانی از بسترهای گوناگون

Privatoria از همـه‌ی دسـتگاه‌ها و بسـترها اعـم از ویـنـدوز، مـک، لینوکس/یونیکـس، فایـر اواس، iOS، و اندرویـد پشـتیبانی می‌کنـد.

7. روش پرداخت ایمن

ایـن کار هیـچ نیـازی بـه درج اطلاعـات شـخصی بـرای ثبت‌نـام ندارد.

8. پشتیبانی فنی زنده

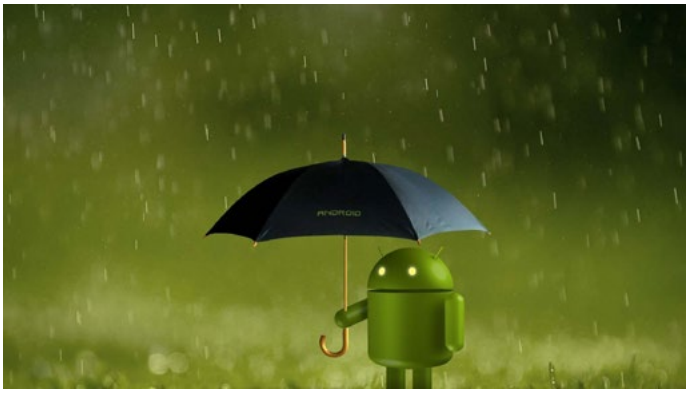
Privatoria امـکان چـت زنـده را نیـز مهیـا می‌سـازد، ایـن قابلیـت در سـاعت کار بـه وقـت اروپـای مرکـزی پشـتیبانی می‌شـود.

9. تضمین برگشت پول

تضمیـن بازگشـت پـول همیشـه موضـوع جالبـی بـوده اسـت، وی‌پـی‌ان Privatoria یـک تضمیـن ۳۰ روزه‌ی برگشـت پـول دارد، یعنـی اگـر ایـن VPN نیازهـای شـما را بـرآورده نکـرد می‌توانیـد درخواسـت بازپرداخـت پـول خـود را بنماییـد.

اخبار عمومی

گوگل می‌گوید پیکسل فون این شرکت به اندازه آیفون امن است



امروزه می‌توان گفت علیرغم سرمایه‌گذاری‌های بسیار از سوی شرکت‌های مختلف به‌منظور امن نمودن محصولاتشان، هیچ دستگاه الکترونیکی به‌طور کامل امنیت ندارد. امنیت یکی از بخش‌های مهمی است که طرفداران سامانه‌های عامل اندروید و iOS درباره آن با هم مناقشه دارند. بسیاری از متخصصان امنیتی بر این باورند که سامانه‌عامل اندروید در حوزه امنیتی واقعاً ضعیف است؛ اما امروزه شاهد این هستیم که گوگل در حال برداشتن قدم‌های بزرگی برای ارتقاء حریم خصوصی و امنیت دستگاه‌هایی است که از این بستر تلفن همراه استفاده می‌کنند.

این غول موتور جستجو حالا راهکاری را برای به‌روزرسانی ماهیانه ارائه کرده است که آسیب‌پذیری‌های کشف شده را وصله می‌کند. در طرف دیگر اکوسیستم iOS امن‌تر است اما دست توسعه‌دهندگان را بیشتر بسته است. نتیجه این‌که شاید نتوانید بهترین‌ها را از هر دو مدل داشته باشید. البته گوگل ادعا می‌کند سامانه‌عامل اندروید به‌زودی امکانات بهتری از همه نظر در اختیار کاربران قرار خواهد داد.

در طی یک مصاحبه، آدریان لودویگ، مدیر امنیتی اندروید گفته است: «به‌طور قطع وقتی صحبت از امنیت باشد، گوگل پیکسل و آیفون هر دو در یک سطح خواهند بود. در بازه زمانی طولانی مدت، محیط متن‌باز اندروید منجر خواهد شد این بستر بهتر از iOS باشد.»

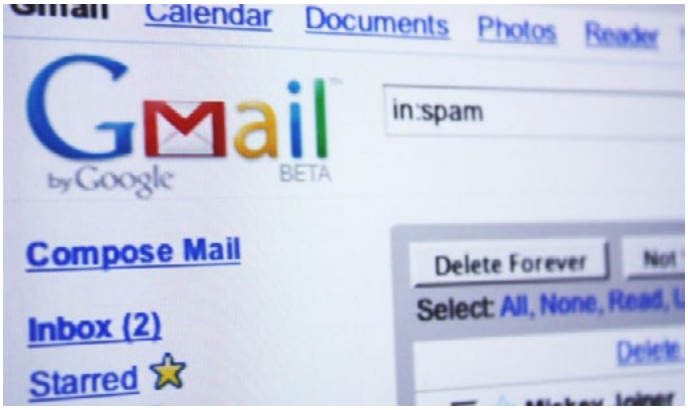
به گفته لودویگ، راهکار امنیتی اندروید با نام Safety Net در حال حاضر ۴۰۰ میلیون دستگاه را پویش می‌کند. به‌علاوه، این محصول می‌تواند حدود ۶ میلیارد برنامه را در روز بررسی کند که خود یک دستاورد عظیم محسوب می‌شود.

وی در ادامه ادعا کرده است به لطف Safety Net امروزه تعداد دستگاه‌های اندرویدی که بدافزار دارند بسیار اندک هستند. او می‌گوید کمتر از ۱ درصد تلفن‌های هوشمند اندرویدی تحت تأثیر PHA ها هستند.

خبر خوب دیگری که لودویگ آن را منتشر کرده است این است که در حال حاضر امنیت اندروید در حدی است که تقریباً برای مهاجمان غیرممکن است تعداد زیادی از دستگاه‌های این سامانه عامل را به‌طور همزمان توسط بدافزار هدف قرار دهند.

اخبار عمومی

نفوذ هوشمندانه به حساب جی‌میل و در دست گرفتن حساب کاربری



هفته‌ی گذشته بود که گوگل یک حفره‌ی امنیتی را در سامانه‌ی احراز هویت جی‌میل وصله کرد. این آسیب‌پذیری به مهاجم اجازه می‌داد حساب کاربری جی‌میل را به سرقت برده و کنترل آن را در دست گیرد. این آسیب‌پذیری توسط احمد مِهتاب که یک محقق امنیتی و مؤسس شرکت Security Fuse است، کشف شد. اجرا کردن این نفوذ بسیار ساده است و کمتر از 10 گام برای انجام آن لازم است.

در این نفوذ از یک آسیب‌پذیری دور زدن احراز هویت و اعتبارسنجی بهره‌برداری می‌شود. این آسیب‌پذیری در یکی از ویژگی‌های جی‌میل وجود دارد که این ویژگی به کاربر اجازه‌ی ارسال رایانامه از حساب کاربری جی‌میل ثانویه را می‌دهد. مِهتاب گفته است این حمله بسیار شبیه به تصاحب حساب کاربری است ولی در این سناریو مهاجم می‌تواند با تایید صاحبِ حساب کاربری، آدرس رایانامه را به سرقت ببرد. با انجام این حمله مهاجم می‌تواند از طریق حساب کاربری آلوده‌شده، رایانامه ارسال کند.

با این حال، این نفوذ یک پیش‌شرط بسیار بزرگ دارد. حساب کاربری جی‌میلی که قرار است هدف قرار بگیرد، باید رایانامه‌های ارسالی از طرف مهاجم را مسدود کرده باشد، یا این حساب غیرفعال شده باشد و یا آدرس مربوط به حسابی باشد که وجود ندارد. تحت این سناریوها مهاجم می‌تواند رایانامه‌هایی با آدرس google@gmail.com و gmail@gmail.com ارسال کند.

گوگل وجود این آسیب‌پذیری‌ها و تلاش برای برطرف کردن آن‌ها را تایید کرده است.

براساس گزارش‌های فنی که توسط این محقق ارائه شده است، به‌نظر می‌رسد این حمله اجازه‌ی دسترسی به محتوای حساب کاربری جی‌میل و سایر سرویس‌های گوگل مثل گوگل درایو و غیره را نمی‌دهد. در نتیجه مهاجم نمی‌تواند به محتوا و اطلاعات شخصی قربانی دسترسی داشته باشد.

این نفوذ مربوط به روشی است که گوگل حساب کاربری اصلی را با آدرس‌های ثانویه پیوند می‌دهد تا قابلیت ارسال و فوروارد رایانامه از حساب‌های دیگر نیز امکان‌پذیر باشد. در این ویدئو مِهتاب نشان داده با چه ترفندی گوگل را وادار می‌کند تا یک حساب رایانامه را به حساب‌های موجود اضافه کند.

برای اجرای این حمله مِهتاب مراحل زیر را دنبال می‌کند.

Gmail's Settings menu---> Send Mail As---> Use Gmail to send from your other email addresses---> Treat as an alias

مِهتاب در ادامه گوگل را مجبور می‌کند برای اضافه کردن این آدرس رایانامه به حساب کاربری در بخش رایانامه‌های ناموجود، رایانامه‌ی تاییدی را ارسال کند که در ادامه یک پیام برگشتی تحویل داده می‌شود. حالا مِهتاب می‌تواند

به این پیام برگشتی دسترسی داشته و شماره کد تایید را بدست آوره و این حساب را با موفقیت به حساب کاربری جی‌میل اضافه کند.

مِهتاب می‌گوید: «هر آدرس جی‌میل که با پروتکل SMTP جی‌میل در ارتباط باشد، در برابر این حفره‌ی امنیتی آسیب‌پذیر است. آدرس‌هایی همچون @gmail.com، @googlemail.com و @googleemail.com. در برخی سناریوها مهاجم می‌تواند قربانی را تحریک کند تا حساب کاربری خودش را غیرفعال کند و یا آدرس رایانامه‌ی مهاجم را مسدود کند. وقتی قربانی این کارها را انجام داد، مهاجم به راحتی می‌تواند حساب کاربری را به سرقت ببرد.»

مِهتاب وجود این اشکال را در تاریخ 20 اکتبر به گوگل اطلاع داد و گوگل نیز همان روز این مشکل را برطرف کرد.

به گفته‌ی مِهتاب نکته‌ی جالب توجه این است که برای گزارش این آسیب‌پذیری مهم، هیچ جایزه‌ای به او داده نشده و فقط نام او در بخش تالار مشاهیر گوگل ثبت شده است.

اخبار عمومی

روند صحیحِ افشای آسیب‌پذیری روز-صفرم چگونه است؟

اوایل هفته‌ی پیش بود که دیدیم گوگل یک آسیب‌پذیری ارتقاء امتیازات محلی در ویندوز 10 را افشاء کرد. این آسیب‌پذیری یک آسیب‌پذیری روز-صفرم است به این معنی که خیلی سریع نمی‌توان مشکل این نوع آسیب‌پذیری‌ها را برطرف کرد. افشاء کردن این آسیب‌پذیری‌ها به‌طور عمومی به مهاجمان این امکان را می‌دهد تا اطلاعات بیشتری از این آسیب‌پذیری کشف کرده و به نفع خود استفاده کنند.

مسئله این‌گونه بوده که یک هفته قبل از آن، گوگل وجود این آسیب‌پذیری را به مایکروسافت خصوصی اطلاع داده بود. گوگل همچنین یک آسیب‌پذیری با شناسه‌ی CVE-2016-7855 مربوط به فلش را به ادوبی هم اطلاع داده بود. در پاسخ به این اطلاعیه‌های صادر شده از طرف گوگل، شرکت ادوبی 5 روز بعد با یک به‌روزرسانی امنیتی این مشکل را برطرف کرد.

این مسئله یک اتفاق خوب برای شرکت ادوبی بود چرا که گوگل در مورد آسیب‌پذیری‌های جدی که قابل بهره‌برداری هستند قانونی دارد بدین شکل که: وجود آسیب‌پذیری به‌طور خصوصی به شرکت مربوطه اطلاع داده می‌شود و اگر این مشکل در عرض 7 روز برطرف نشود، آسیب‌پذیری مورد نظر به‌طور عمومی افشاء می‌شود. حال ببینیم دلیل گوگل برای چنین قانونی چیست؟

«ما معتقدیم که برای برطرف کردن آسیب‌پذیری جدی و مهم، در عرض 7 روز می‌توان عملیات ضروری را انجام داد. دلیل ما هم برای این تصمیم این است که هر روزی که یک آسیب‌پذیری مهم و قابل بهره‌برداری، وصله‌نشده باقی بماند، احتمال اینکه تعداد رایانه‌های آلوده افزایش یابد، بیشتر می‌شود.»

دلیل گوگل برای نگرانی بسیار منطقی بود چرا که مایکروسافت قبلا فهمیده بود قبل از افشاء آسیب‌پذیری توسط گوگل، یک گروه APT روسی با نام Fancy Bear از این آسیب‌پذیری روز-صفرم در حملات خود بهره‌برداری می‌کردند.

مایکروسافت هنوز برای این آسیب‌پذیری وصله‌ای منتشر نکرده ولی در پست وبلاگی اعلام کرده که در وصله‌های روز سه‌شنبه در تاریخ 8 نوامبر، وصله‌ی این آسیب‌پذیری در دسترس خواهد بود.

امّا روند منطقی و عادی افشای آسیب‌پذیری چگونه است؟

در حوزه امنیت اطلاعات توافق استانداردی برای افشای آسیب‌پذیری‌ها وجود ندارد. بسیاری از شرکت‌ها «افشای مسئولانه» را رعایت می‌کنند به این معنی که ابتدا آسیب‌پذیری را همراه با جزئیات کامل به شرکت مورد نظر به‌طور خصوصی اطلاع می‌دهند و پس از اینکه

آن آسیب‌پذیری وصله شد، جزئیات آن را عمومی منتشر می‌کنند.

معمولاً کسانی که آسیب‌پذیری را کشف کرده‌اند برای وصله‌ی آن نیز با شرکت مربوطه همکاری می‌کنند. تا زمانی که شرکت مربوطه با نهایت حسن‌نیت برای رفع آسیب‌پذیری تلاش می‌کند، برای افشای عمومی آن هفته‌ها و یا ماه‌ها فرصت داده می‌شود ولی برخی‌ها نیز برای برطرف کردن آسیب‌پذیری مهلت تعیین می‌کنند. مثلاً گوگل 60 روز مهلت را پیشنهاد داده است در حالی‌که ممکن است بقیه فرصت بیشتری بدهند.

در حوزه‌ی امنیت اطلاعات همه با این قوانین و اصول افشای مسئولانه موافق نیستند. شاید خیلی جسورانه به نظر برسد ولی برخی معتقدند هرچه سریع‌تر باید آسیب‌پذیری را به اطلاع عموم رساند بخصوص وقتی که این آسیب‌پذیری به‌طور فعال قابل بهره‌برداری باشد. وقتی گوگل به دو شرکت ادوبی و مایکروسافت برای برطرف کردن آسیب‌پذیری‌ها 7 روز مهلت داد، ممکن است بقیه فکر کرده باشند که این مهلت مناسبی برای برطرف کردن چنین آسیب‌پذیری نیست.

ایده‌ای که پشت افشای سریع آسیب‌پذیری‌ها وجود دارد این است که آن شرکت تحت فشار جمعی قرار گرفته و موظف می‌شود با جدیت تمام برای رفع آسیب‌پذیری تلاش کند، مخصوصاً اگر این شرکت در آسیب‌پذیری‌هایی که قبلا افشاء شده، مسئولانه و جدی عمل نکرده باشد. با این حال باید به این نکته نیز توجه داشت که این رویکرد در برخی موارد می‌تواند نتیجه‌ی عکس داشته باشد و راه حمله برای مهاجمان بالقوه باز شود. همچنین برای شرکت مربوطه نیز می‌تواند نتیجه‌ی عکس داشته باشد اگر هرچه سریع‌تر به این آسیب‌پذیری رسیدگی نکند.

آیا شما هم فکر می‌کنید که افشای سریع آسیب‌پذیری‌ها حرکتی بی‌پروایانه است یا این کار، کارِ درستی است؟ آیا حق با گوگل بوده است؟

اخبار عمومی

باج‌افزار Cerber در کمین پایگاه داده‌ها

عوامل باج‌افزار بسیار قوی Cerber در حال حاضر علاوه بر افراد، شرکت‌های تجاری را نیز با ماژولی که پایگاه داده‌ها را رمزنگاری می‌کند، هدف قرار داده‌اند.

در ماه جولای که این باج‌افزار مورد بررسی قرار گرفت بیش از 150 پویش داشت که 150,0000 کاربر را هدف قرار داده بود و در طول آن ماه با کسب 195هزار دلار سود، رکورد زد. از این مبلغ 78هزار دلار عاید توسعه‌دهندگان این باج‌افزار شد.

تخمین زده می‌شود عوامل پشت این باج‌افزار در سال 1 تا 2.5 میلیون دلار سود به جیب بزنند.

محقق امنیتی Matthew Rosenquist می‌گوید تکامل بعدی این باج‌افزار هدف قرار دادن شرکت‌های تجاری است. این محقق می‌گوید این باج‌افزار در حال حاضر در حال متوقف کردن فرآیندهای در حال اجرا مربوط به پایگاه داده و در ادامه رمزنگاری داده‌های داخل آن است. این تغییر تمرکز از افراد به سمت شرکت‌ها یک تغییر مهم و قابل توجه است چرا که پایگاه داده‌ها حاوی داده‌های مهم و عملیاتی هستند. وقتی پایگاه داده باز است و توسط کاربران استفاده می‌شود، رمزنگاری داده‌های آن آسان نیست.

مسلماً این باج‌افزار تنها تهدید برای سازمان‌ها نیست. قبلاً هم باج‌افزارهای خصوصی و خاص‌منظوره مشاهده شده که سازمان‌های بسیار بزرگ را هدف قرار داده و میلیون‌ها باج برای ارائه‌ی کلید رمزگشایی درخواست کرده‌اند.

این محقق امنیتی به مدیران سامانه هشدار داده که به توقف‌های ناگهانی پایگاه داده اهمیت دهند چرا که می‌تواند نشانه‌ای از رمزنگاری داده‌ها توسط باج‌افزار Cerber باشد.

به نظر می‌رسد که روشی برای رمزگشایی پرونده‌هایی که با Cerber رمزنگاری شده‌اند وجود ندارد و به‌روزرسانی که بر روی ابزار رمزگشایی CheckPoint انجام شده، تاثیری نداشته است.

محققان امنیتی در تلاش هستند ضعفی در پیاده‌سازی یا آسیب‌پذیری در این باج‌افزار پیدا کرده و بتوانند آن را رمزگشایی کنند.

فصل دوم

مدیریت امنیت

مدیریت امنیت

فیس‌بوک موافق توقف طرح «استفاده از داده‌های کاربران واتس‌اپ برای تهیه‌ی تبلیغات هدف‌مند»

در ماه آگوست، فیس‌بوک از یک برنامه‌ی بسیار بحث‌برانگیز برای برداشت داده‌ها از پیام‌رسان واتس‌اپ خود و ارائه‌ی تبلیغات مرتبط بیشتر با این شبکه‌ی اجتماعی صحبت به میان آورد.

بسیاری از کاربران با این حرکت موافق نبودند، زیرا هیچ راه حل انتخابی در کار نبود، کاربران واتس‌اپ می‌بایست این برنامه را به سرعت می‌پذیرفتند، و حتی اگر کاربران آن را انتخاب نمی‌کردند هم برخی از داده‌هایشان به اشتراک گذاشته می‌شد.

در نهایت، برخی کشورها مانند بریتانیا ایستادگی کرده و با این تصمیم مخالفت کردند.

اداره‌ی کمیسر اطلاعات انگلستان از فیس‌بوک و واتس‌اپ درخواست کرد تا به نحوی بهتر این تغییرات را برای کاربران خود در انگلستان تشریح کنند و اگر چنین کاری انجام ندهند، این اداره‌ی جریمه‌ی سنگینی را برایشان در نظر بگیرد.

خبر خوب چیست؟

در پاسخ به این حواشی، این غول رسانه‌های اجتماعی موافقت کرد تا به اشتراک‌گذاری «داده‌ها» میان فیس‌بوک و واتس‌اپ را در بریتانیا متوقف کند تا فقط آگهی‌های تبلیغاتی موجود روی خود این شبکه‌ی اجتماعی را ادامه دهد؛ این داده‌ها شامل شماره‌ی تلفن کاربران می‌باشد.

کمیسر اطلاعاتی، الیزابت دنم گفت: «ما در حال حاضر از فیس‌بوک و واتس‌اپ خواسته‌ایم تا تعهدی را برای توضیح بیشتر به کاربران به امضاء برسانند، تعهدی که در مورد این‌که چگونه از اطلاعات کاربران استفاده خواهد شد، و نیز اعطای کنترل مداوم روی این داده‌ها به کاربران تنظیم شده است.»

وقتی فیس‌بوک در اواخر فیس‌بوک از این معاهده خبر داد، دنم گفت که تغییرات احتمالی روی قوانین حفاظت اطلاعات انگلستان را بررسی خواهد کرد، و هم‌اکنون یک به‌روزرسانی را منتشر کرده که نشان می‌دهد این غول شبکه‌های اجتماعی، یعنی فیس‌بوک، با منع به اشتراک‌گذاری داده‌های کاربران در انگلستان موافق است.

دنم گفت که این حق کاربران است که روی اطلاعات خودشان کنترل داشته باشند، وی در حال حاضر از فیس‌بوک و واتس‌اپ خواسته تا به کاربران اجازه دهد تا دسترسی به داده‌هایشان را در ۳۰ روز باقی‌مانده محدود سازند، و به آن‌ها اجازه دهد هر وقت که خواستند این شرایط را نقض کنند.

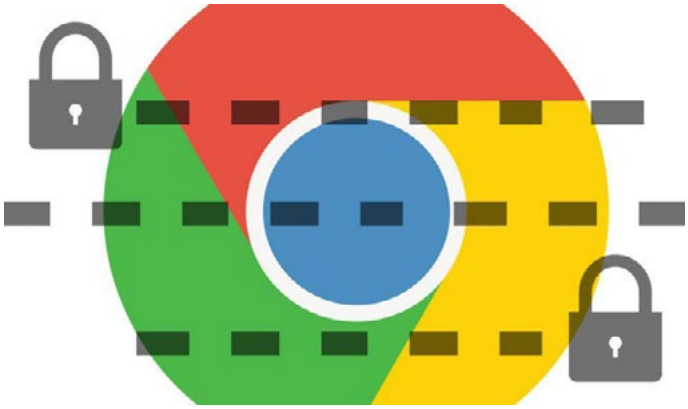
وقتی که فیس‌بوک در سال ۲۰۱۴ در ازای ۱۹ میلیون دلار فیس‌بوک را خریداری کرد، کاربران نگران این مطلب بودند که تعهدات این شرکت منجر به حفظ حریم خصوصی‌شان نشود. ولی واتس‌اپ به آن‌ها اطمینان داد که حریم خصوصی آن‌ها به هیچ وجه دستخوش آسیب قرار نخواهد گرفت.

امـا اندکـی بعـد از انجـام ایـن معاملـه، کاربـران واتـس‌اپ احسـاس کردنـد کـه ایـن پیام‌رسـان محبـوب بـه آن‌هـا خیانـت کـرده اسـت.

واتـس‌اپ بعـد از معرفـی رمزگـذاری پایـان بـه پایـان، بـه یکـی از محبوب‌تریـن پیام‌رسـان‌های ایمـن تبدیـل شـد، ولـی ایـن تحـول در حریـم خصوصـی‌اش باعـث شـد کـه برخـی از کاربران تغییـر رویـه داده و برنامه‌هـای امن‌تـری ماننـد تلگـرام یـا سـیگنال را بـرای ادامـه‌ی کار خـود انتخـاب کننـد.

مدیریت امنیت

نیمی از صفحات در کروم با HTTPS به نمایش درمی‌آیند



در ابتدای امر توسط موزیلا، و در آخر از سوی گوگل تأیید شد که رمزگذاری در حال تبدیل به یک بلوک ساختمانی استاندارد برای وب‌گاه‌ها و برنامه‌های کاربردی است.
گوگل روز گذشته گزارش داد که بیش از نیمی از صفحات بارگذاری شده در نسخه‌های رومیزی مرورگر کروم توسط HTTPS به نمایش درمی‌آیند.
گوگل، در گزارش شفاف‌سازی خود که برای اولین بار آمار و ارقام مربوط به استفاده از HTTPS را نیز شامل شده است، گفت: «مرور ایمن وب به وسیله‌ی HTTPS به یک هنجار تبدیل شده است.»
دو هفته پیش، موزیلا بیان داشت که برای اولین بار از زمان شروع نظارت خود متوجه شده که نیمی از کل ترافیکِ در حال انتقال، رمزگذاری شده است. این رقم از دسامبر ۲۰۱۵ حدود ۱۰ درصد رشد داشته است. این افزایش به خاطر انفجار مراجع رایگان صدور گواهی‌نامه‌ی دیجیتال و سرویس‌های مجوزهای SSL، همچون مواردی است که توسط Let's Encrypt، آمازون، Cloudflare، وردپرس و غیره ارائه شده‌اند.
گوگل در بسترهای مختلفی در جای جای جهان بارگذاری می‌شود. گوگل گفت که از ۳۱ اکتبر حدود ۵۳ درصد از محتوای صفحات بارشده روی سامانه‌های تحت ویندوزی که از کروم استفاده می‌کنند، از طریق HTTPS مهیا شده‌اند؛ سامانه‌های لینوکس ۵۷ درصد، سامانه‌های مک ۶۲ درصد، و سامانه‌های کروم حدود ۶۸ درصد را به خود اختصاص داده‌اند. در آخرین رتبه اندروید با ۴۲ درصد قرار دارد، البته این رقم از ۲۹ درصد در ماه مارس ۲۰۱۵ به این مقدار رسیده است.
آدرین پورتر فلت و امیلی شکتر از تیم امنیتی کروم گفتند: «ما به کارمان ادامه می‌دهیم تا مطمئن شویم مهاجرت به HTTPS به بهبود امنیت منجر می‌شود.»
گوگل به وب‌گاه‌های HTTPS رتبه‌های جست‌وجوی مطلوبی را به عنوان پاداش اعطاء می‌کند، به این امید که سرعت تبدیل به یک بستر وب رمزشده را افزایش دهد.
محققان گوگل همچنین اشاره کردند که ترافیک ارائه‌شده توسط HTTPS در حال افزایش است، و آگهی‌های برخاسته از منابع گوگل همچون AdSense، AdWords و سایرین از HTTPS پشتیبانی می‌کنند، و این آگهی‌ها به‌طور مستقیم از طریق شبکه‌های تبلیغاتی شخص ثالث که بایست «HTTPS-پسند» باشند، به فروش می‌رسند.
آمار گوگل بیان می‌کنند که کاربران زمان بیشتری را صرف صفحات HTTPS می‌کنند، آمار ۶۹ درصد و ۷۰ درصد به ترتیب به کاربران ویندوز و مک اشاره دارد. از نظر جغرافیایی آمریکا مقام نخست استفاده از HTTPS را در محیط ویندوز داراست، سپس ترکیه، روسیه، مکزیک و سایرین ۵۰ درصد کاربران HTTPS را پوشش می‌دهند. با این حال رشد ژاپن بسیار کندتر است، تنها ۳۵ درصد از آمار را شامل می‌شود. از نظر نقش ارائه‌دهندگان SSL

رایگان، به نظر می‌رسد Let's Encrypt جلودار باشد،Let's Encrypt در یک هفته‌ی اخیر یک میلیون گواهی دیجیتال را منتشر نموده است، و در طول این سال میلادی حدود ۷ میلیون گواهی را صادر کرده است.

مدیریت امنیت

جاسوس‌افزاری با نام Exaspy مدیران رده‌بالا را هدف قرار داده است

محققان می‌گویند جاسوس‌افزار اندرویدی را با نام Exaspy کشف کرده‌اند که به‌عنوان یک کالا فروخته می‌شود و از مدیران رده‌بالا جاسوسی می‌کند. به گفته‌ی آزمایشگاه تحقیقاتی Skycure این بدافزار به‌عنوان سرویسی ماهانه 15 دلار فروخته می‌شود و تقریباً تمامی ارتباطات تلفنی از جمله تماس‌های تلفنی، پیام‌ها، اسکایپ و تصاویر را می‌تواند شنود کند.

Skycure گفته است این جاسوس‌افزار را ماه سپتامبر کشف کرده زمانی که یکی از مشتریان آن بر روی یک تصویر اجرایی، یک برنامه‌ی جعلی با نام Google Services را در حال اجرا شناسایی کرده است. محققان می‌گویند کسانی که هدف این جاسوس‌افزار قرار گرفته‌اند افرادی با رده‌های بالای اجرایی در شرکت‌های فناوری بزرگ هستند. این جاسوس‌افزار تنها بر روی بستر اندورید سازگار است و برای نصب آن نیاز است تا مهاجم به تلفن همراه قربانی دسترسی فیزیکی داشته باشد. پس از اینکه Exaspy نصب شد با تغییر نام خود به Google Services تلاش می‌کند خودش را مخفی کند. به گفته‌ی محقق این آزمایشگاه، این بدافزار هنوز توسط پویشگرهای امنیتِ موبایل تشخیص داده نشده است.

این جاسوس‌افزار پس از نصب شدن می‌تواند دستورات شِل را اجرا کند و یا شِل معکوس را ایجاد کند تا از طریق آن امتیازات برنامه با بهره‌برداری‌های خاصی که در بسته‌ی اصلی وجود ندارد، بالا برود.

بستری که پشت Exaspy وجود دارد یک کارگزار دستور و کنترل است که پرونده‌های محلی همچون رایانامه‌ها، تصاویر و ویدئوها را منتقل کرده و بر آن‌ها نظارت می‌کند و برای اجرای دستورات شِل استفاده می‌شود.

Exaspy داخل وب‌تاریک مخفی نشده است ولی هنوز یک جاسوس‌افزار ناشناخته است. ویژگی منحصربفرد این جاسوس‌افزار این است که مهاجم برای نصب آن باید به تلفن همراه دسترسی فیزیکی داشته باشد. این بدافزار به مجوزهای کامل مدیر سامانه نیاز دارد همچنین برای فعال‌سازی و نصب خود به‌عنوان بسته‌های سامانه‌ای به شماره مجوزهایی نیاز دارد تا حذف کردن خود از روی سامانه‌ی قربانی را سخت‌تر کند.

این جاسوس‌افزار خود را به‌جای برنامه‌ی Google Services جا می‌زند تا زمانی‌که این بدافزار در حال اجرا شدن است، کاربر گمراه شده و تصور کند برنامه‌ی گوگل در حال اجراست.

ویژگی دیگر این جاسوس‌افزار ارتباط با کارگزارهایی است که بر روی سرویس ابر گوگل میزبانی می‌شوند و بارگیری از آدرس URL هارکدشده‌ی hxxp://www[.]exaspy[.]com است.

از مدت‌ها پیش جاسوس‌افزارهایی برای بسترهای اندروید و iOS وجود داشته است. با این وجود چند نمونه‌ی سطح بالا از این جاسوس‌افزارها که با حملاتی پیچیده، مدیران

رده‌بالا را هدف قرار داده، نگران‌کننده است. افشاگری‌های اخیر در مورد جاسوس‌افزار iOS با نام Pegasus که در دفاع از حقوق بشر تلاش می‌کرد، نشان می‌دهد نگرش‌های بی‌پروایانه در استفاده از جاسوس‌افزارها علیه افراد مهم، در حال رشد است.

آزمایشگاه تحقیقاتی Skycure به راه‌حل‌های پیشگیری و کاهش این‌گونه جاسوس‌افزارها اشاره کرده است:

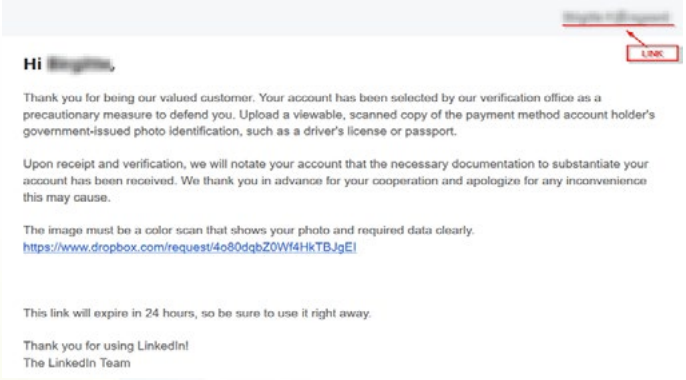
- از پین کد و احراز هویت با اثرانگشت برای دسترسی به تلفن همراه خود استفاده کنید.
- عیب‌یابی از طریق USB را غیرفعال کنید.
- دائماً فهرست مدیریتی تلفن همراه خود را بررسی کرده و مؤلفه‌هایی که به آن‌ها اعتماد ندارید را غیرفعال کنید.

مدیریت امنیت

دردسری دیگر برای لینکدین: پویش جدید فیشینگ

حملات فیشینگ همچنان ادامه داشته و در حال تبدیل به یک تهدید جدی هستند. مهاجمان نیز از راه‌های مختلفی همچون شبکه‌های اجتماعی و برنامه‌های تلفن همراه در تلاش هستند تا اطلاعات کاربران را به سرقت ببرند. براساس گزارش نقض داده‌ی Verizon که در سال 2015 منتشر شده، 23 درصد از گیرنده‌ها، رایانامه‌های فیشینگ را باز کرده و 11 درصد بر روی ضمیمه‌های آلوده کلیک می‌کنند.کارشناسان شرکت امنیتی Heimdal گزارش دادند پویش فیشینگی مشاهده شده که قصد جمع‌آوری اطلاعات محرمانه‌ی کابران بی‌گناه را دارد.

بردار حمله در این پویش رایانامه‌ای به شکل زیر است:



Hi [redacted],

Thank you for being our valued customer. Your account has been selected by our verification office as a precautionary measure to defend you. Upload a viewable, scanned copy of the payment method account holder's government-issued photo identification, such as a driver's license or passport.

Upon receipt and verification, we will notate your account that the necessary documentation to substantiate your account has been received. We thank you in advance for your cooperation and apologize for any inconvenience this may cause.

The image must be a color scan that shows your photo and required data clearly.
https://www.dropbox.com/request/4o80dqbZ0Wf4HkTBJgEI

This link will expire in 24 hours, so be sure to use it right away.

Thank you for using LinkedIn!
The LinkedIn Team

صبر کنید! چیزی که می‌بینیم عجیب است. لینکدین از ما می‌خواهد که پرونده‌هایی را برایش ارسال کنیم؟ لینکدین می‌خواهد از طریق اسنادی که ما برایش ارسال کردیم، هویت ما را تایید کند؟

متاسفانه بسیاری از کاربران بی‌اطلاع و ناآگاه در دام این کلاهبرداری‌ها می‌افتند.

این رایانامه از کاربر رسید پرداخت را درخواست می‌کند و کاربرانی که عضو ویژه (پولی) لینکدین هستند ممکن است وسوسه شده و اطلاعات پرداخت خود را ارسال کنند.

بیایید دقیق به آدرس فرستنده‌ی رایانامه نگاه کنیم:

postmaster [@] fnotify.com

بسیار واضح است که این رایانامه از سمت یک شبکه‌ی رسانه‌ای حرفه‌ای فرستاده نشده است.

دامنه‌ای که توسط عاملان حمله‌ی فیشینگ استفاده شده (http : [//]fnotify.com/) یک وب‌گاه خالی وردپرس است و احتمالاً یک وب‌گاه آلوده بوده که در این پویش فیشینگ بکار گرفته شده است.یک مورد شک‌برانگیز دیگر در این رایانامه زمان محدودی است که مشخص شده است. این ترفند در حوزه‌ی مهندسی اجتماعی بسیار شناخته‌شده است تا کاربر را وادار به اجرای دستورات کنند.

حالا بیایید پیوند قرار گرفته در گوشه‌ی سمت راست-بالا را بررسی کنیم که یک صفحه‌ی تنظیم مجدد گذرواژه است که با HTTPS امن شده است. می‌توان حدس زد که این پیوند برای فریب کاربر قرار داده شده تا کاربر با مراجعه به این صفحه و مشاهده‌ی امن بودن آن مطمئن شود که این رایانامه قانونی است.

اگر با چنین رایانامه‌ی فیشینگی مواجه شدید، این شرکت توصیه کرده تا این قضیه را از طریق رایانامه‌ی phishing@linkedin.com اطلاع دهید.

مدیریت امنیت

تعلیق تمامی تراکنش‌های برخط در پی ِ سرقت مجازی از بانک Tesco

پس از یک دزدی مجازی که هزاران نفر از مشتریان را تحت تاثیر قرار داد، بانک Tesco تمامی تراکنش‌ها را متوقف کرد. تحقیقات هنوز در حال انجام است.

این بانک در اقدامی برای متوقف کردن این حمله‌ی مجازی، تمامی تراکنش‌های مشتریان را متوقف کرده است. این اقدام توسط بنی هیگینز مدیر اجرایی این بانک اعلام شد. این بانک اعلام کرده که در طول این آخر هفته به حساب کاربری 40 هزار نفر از 136هزار مشتری نفوذ شده است و متاسفانه 50 درصد از این مشتریان موجودی خود را از دست داده‌اند.

بانک Tesco از سال 2008 تحت مالکیت Tesco PLC بوده و نزدیک به 7.8 میلیون حساب کاربری دارد. این بانک تایید کرده که فعالیت‌های مشکوکی را اواخر شنبه و اوایل صبح یکشنبه شناسایی کرده است.

هیگینز گفت: «ما بخاطر ناراحتی و نگرانی که برای مشتریانمان بوجود آمده بسیار عذرخواهی می‌کنیم و تحت فشار بسیار بالایی مراحل حفاظت از مشتریان خود را دنبال می‌کنیم. در یک اقدام احتیاطی تصمیم گرفتیم تا امروز موقتاً تراکنش‌های برخط حساب‌های کاربری را متوقف کنیم.»

این حادثه بخاطر تعداد بالای ِ مشتریانی که تحت تاثیر قرار گرفته‌اند و همچنین به‌خاطر اقدامی که توسط این موسسه مالی برای پیشگیری از این حمله اتخاذ شده است، در ذهن باقی خواهد ماند.

این بانک مقدار پولی که از حساب‌های مشتریان به سرقته رفته را بسیار کم گزارش کرده است. به هرحال بانک تمامی ضرر و زیان‌های ناشی از این حمله را به مشتریان پرداخت کرده و بخاطر پشتیبانی ضعیف در پاسخگویی به پیگیری‌های مشتریان عذرخواهی کرده است.

یکی از مشتریان این بانک در توییتی گفته است که موجودی او 700 پوند کاهش پیدا کرده در حالی‌که هیچ تراکنشی انجام نداده است. متن توییت بدین شکل است: «به حساب کاربری ما نفوذ شده است. تمامی پول‌های ما به باد رفته و هیچ متن و رایانامه‌ای دریافت نکرده‌ایم. هیچ کس از طرف Tesco تاکنون پاسخگو نبوده است.»

در حالی‌که محققان امنیتی در تلاش هستند تا عاملان این حمله را شناسایی کنند، مدیر اجرایی این بانک از عنوان عاملان احتمالی این قضیه امتناع کرده است.

هیگینز گفت: «در دنیای مدرن کنونی تسخیرناپذیری غیرممکن است. ما در خصوص این حادثه با آژانس جرائم بین‌المللی و سازمان مالی در حال مذاکره هستیم.»

فصل سوم

امنیت سایبری

امنیت‌سایبری

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

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

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

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

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

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

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

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

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

یکی از رایانامه‌هایی که به بیرون درز کرده نشان می‌دهد که هزینه‌ی مراسم ازدواج چلسی کلینتون، دختر هیلاری و بیل، از بنیاد کلینتون تأمین شده است.

امنیت‌سایبری

چین در پی تصویب قوانین سخت‌گیرانه‌تر برای سانسور اینترنت

مدت مدیدی است که نام چین به خاطر سیاست‌های سخت‌گیرانه‌ای که در زمینه‌ی سانسور وضع کرده، بر سر زبان‌ها افتاده است؛ این سخت‌گیری موجب شده که شرکت‌های خارجی دیگر نتوانند به راحتی با این پرجمعیت‌ترین کشور جهان که بالغ بر ۱,۳۵ میلیارد نفر جمعیت دارد، به تجارت بپردازند.

در حال حاضر، دولت چین مقررات امنیت سایبری بحث‌برانگیز جدیدی را وضع کرده که باعث تشدید شرایط سانسور در این کشور شده است، به این ترتیب شرکت‌های فن‌آوری برای ادامه‌ی کسب و کار خود در این کشور با مشکل جدی مواجه شده‌اند.

این قانون، که روز دوشنبه به اطلاع عموم رسیده و در ژوئن ۲۰۱۷ اجرا خواهد شد، با هدف مبارزه با تهدیدات رو به رشدی مانند نفوذ سایبری و تروریسم به تصویب رسیده است، اما در حقیقت با محلی‌سازی داده‌ها، الزامات استفاده از اسامی حقیقی، و نظارت همراه است.

این قانون امنیت سایبری مستلزم استفاده از سرویس‌های پیام‌رسان فوری و سایر عوامل اینترنتی است تا کاربران را مجبور به ثبت‌نام با اسامی حقیقی و اطلاعات شخصی‌شان نماید، این موضوع گم‌نامی کاربر در فضای برخط را به چالش می‌کشد.

این قانون پیشنهادی همچنین شامل الزاماتی برای «محلی‌سازی داده‌ها» است که باعث می‌شود «عوامل زیرساختی اطلاعات حیاتی» اطلاعات مربوط به کاربران خود را در محدوده‌ی مرزهای کشور خود ذخیره نمایند، مشابه همان قانونی که دولت روسیه به شرکت‌های فن‌آوری خارجی تحمیل کرده است.

دیده‌بان حقوق بشر چین (HRW)، مخالف این قانون است؛ HRW می‌گوید که این قانون شامل هیچ تعریف دقیقی برای عوامل زیرساختی نمی‌باشد، و منجر به گسترش کنترل دولت روی رسانه‌هایی می‌شود که در حال حاضر به شدت تحت نظارت و سانسور قرار دارند.

علاوه بر این، این قانون تازه برخی از شرایط جدید برای امنیت سایبری را نیز پوشش می‌دهد، و شرکت‌ها را مجبور به ارائه‌ی «پشتیبانی فنی» برای سازمان‌های دولتی می‌کند تا به این وسیله بتوانند تحقیقات مربوط به جرایم و امنیت ملی را صورت داده و به سانسور محتوایی بپردازند که «ممنوع» می‌باشند.

اگرچه این پشتیبانی فنی به وضوح در قانون جدید تعریف نشده است، محققان بر این باورند که مقامات می‌توانند از شرکت‌ها بخواهند که در پشتی‌های رمزنگاری یا سایر کمک‌های نظارتی را تحت پوشش «پشتیبانی فنی» در اختیارشان بگذارند.

به موجب این قانون، شرکت‌ها و عوامل دست‌اندرکار شبکه‌ها بایست «رخدادهای امنیتی» را به دولت گزارش کنند و کاربران را در جریان نقض داده‌ها قرار دهند.

قوانینی که به «سرنگونی نظام سوسیالیستی»، «ساخت و

اشاعه‌ی اطلاعات نادرست برای بر هم زدن نظم اقتصادی»، و نیز ایجاد موج «جدایی‌طلبی یا آسیب رساندن به وحدت ملی» منجر می‌شوند، به عنوان قوانین مجرمانه‌ی زیرمجموعه‌ی این قانون تازه معرفی می‌شوند.

چنین الزاماتی باعث ایجاد نگرانی‌های جدی برای کاربران و شرکت‌هایی شده که در چین فعالیت می‌کنند، کشوری که اینترنت و آزادی برخط به شدت توسط دولت سانسور می‌شود.

امنیت‌سایبری

نتیجه‌ی انتخابات ریاست‌جمهوری آمریکا، خبری ناخوشایند برای اپل و مایکروسافت

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

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

حماسه‌ی سن برناردینو

علاوه بر این، ترامپ اغلب موارد مشابه با اپل و مایکروسافت را به خاطر این‌که در فقره‌های بحث‌برانگیز مانند آیفونِ حادثه‌ی سن‌برناردینو تحت قوانین آمریکا فعالیت نمی‌کنند، محکوم کرده است؛ همان‌طور که در خبرها گفتیم، در این حادثه FBI از اپل خواسته بود تا به تلفن یکی از تیراندازان دسامبر ۲۰۱۵ پیدا کند.

اگرچه اپل به شدت با این درخواست مخالفت کرد و متعهد شد که حریم خصوصی بی‌عیب و نقصی را به کاربران خود ارائه کند، و به هویت آن‌ها کاری نداشته باشد، اما برخی از مقامات رسمی این شرکت را مورد بمباران سرزنش‌های خود قرار دادند، این مقامات می‌گویند که اپل امنیت ملی را زیر سؤال برده و از تروریست حمایت می‌کند. بدیهی است که ترامپ یکی از همین منتقدان بوده، وی با کلمات بسیار تند و تیزی ادعا می‌کرد که اگر در مقام ریاست‌جمهوری بود هرگز اجازه نمی‌داد اپل دست به چنین کاری بزند.

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

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

تحریم اپل و در پشتی‌ها

ترامپ گفت: «اپل باید امنیت این گوشی را فراهم کند، خب؟ من تصور می‌کنم شما بایست تا زمانی که اپل شماره‌ی امنیتی این گوشی را ارائه کند، محصولات آن را تحریم کنید. من فقط به این موضوع فکر می‌کنم: تحریم اپل!»

اگر تا این‌جای کار برایتان عجیب نبود بد نیست بدانید

که ترامپ به اینترنت روی آورده تا اپل را به خاطر سرباز زدن از نفوذ به تلفن این تروریست محکوم کند، اما سرزنش‌های خود را با یک آیفون در توییتر ثبت کرده است!

این راز بر کسی پوشیده نیست که این غول‌های فن‌آوری در مبارزه علیه دولت آمریکا با یک‌دیگر متحد بودند و در پاره‌ای از موارد تصمیماتی را اتخاذ نمودند که به‌طور مستقیم روی وضعیت ترامپ تأثیر می‌گذاشت.

به‌طور مثال مایکروسافت حاضر به حمایت مالی از کنوانسیون ملی جمهوری‌خواهان نشد، و در عوض تصمیم گرفت در عرصه‌ی فن‌آوری مشارکت داشته باشد.

برخی از شرکت‌های دیگر از جمله اپل و گوگل به پیروی از مایکروسافت به کار خود ادامه دادند؛ روشن است دونالد ترامپ دل خوشی از آن‌ها نداشته باشد.

ترامپ در طول مبارزات انتخاباتی خود بارها و بارها خاطرنشان کرد که تمایل دارد شرکت‌های آمریکایی روی تأسیسات آمریکا تمرکز کنند و نیروی کار آمریکایی را به خدمت بگیرند، این در حالی است که هزاران نفر از کارکنان مایکروسافت، اپل، گوگل و سایرین در خارج از مرزهای این کشور فعالیت می‌کنند، جالب است که از این به بعد ببینیم این روابط چگونه متحول خواهد شد.

دونالد ترامپ در سخنرانی اخیر خود وعده داد که رئیس‌جمهور تک‌تک آمریکایی‌ها خواهد بود و برای این‌که آمریکا مجدداً به قدرت برسد خواهد جنگید.

امنیت‌سایبری

روسیه از امریکا می‌خواهد درباره گزارش نفوذ اخیر توضیح دهد

منابع خبری می‌گویند مسکو از واشنگتن خواسته است درباره گزارش اخیر منتشر شده شامل نفوذ به روسیه توضیح دهد. در این گزارش آمده بود که ارتش امریکا توانسته است به زیرساخت‌های حساس روسیه نفوذ کرده و در نظر دارد از این نفوذ به‌منظور اقدام تلافی‌جویانه در برابر خرابکاری احتمالی روسیه در انتخابات بهره‌برداری کند.

NBC روز جمعه گفته بود طبق مصاحبه‌ای که با یکی از مقامات ارشد سازمان اطلاعات انجام داده است نفوذگران ارتش امریکا توانسته‌اند به شبکه‌های ارتباطی، توزیع برق و ستاد فرماندهی کرملین نفوذ کنند. این نفوذها در صورت لزوم می‌توانند به حمله به سامانه‌های مذکور کمک کنند.

در پاسخ به این گزارش، وزارت امور خارجه روسیه از مقامات امریکایی خواسته است توضیحاتی را ارائه کنند. در بیانیه منتشرشده از سوی روسیه آمده است: «اگر پاسخی از سوی مقامات امریکایی دریافت نکنیم این بدان معناست که فعالیت‌های خرابکارانه و تروریستی سایبری از سوی دولت مذکور هدایت می‌شوند. در صورت وقوع حادثه مسکو این حق را کاملاً برای خود مسلم می‌داند که دولت امریکا را متهم کند.»

در پی یک سری حملات سایبری نسبت داده شده به روسیه از جمله حمله علیه سامانه‌های حزب دموکرات امریکا و پایگاه‌داده ثبت‌نام رأی‌دهندگان، مقامات امریکایی به‌طور رسمی روسیه را به‌عنوان مقصر اصلی این حملات معرفی کردند. آن‌ها گفته بودند که دولت روسیه قصد ایجاد تداخل در انتخابات امریکا را دارد. به‌علاوه مقامات امریکایی گفته بودند در اقدامی در زمان مناسب پاسخ روسیه را خواهند داد.

روسیه اتهامات وارد شده را رد کرده و آن‌ها را عوام‌فریبی و کاملاً غیرواقعی خوانده بود.

سخنگوی کاخ کرملین، دمیتری پسکوف می‌گوید: «تهدیدهای مطرح شده علیه مسکو کاملاً غیرقابل قبول هستند چرا که در مقام معاون رئیس‌جمهور امریکا مطرح شده‌اند.»

Guccifer 2.0، همان نفوذگری که ادعا کرده بود حملات سایبری علیه حزب دموکرات را انجام داده است گفته بود انتخابات امریکا را رصد می‌کند. او از سایر نفوذگران خواسته بود انتخابات را «از داخل سامانه» رصد کنند.

برخی متخصصان امنیتی معتقدند Guccifer 2.0 شخصیتی ساختگی از سوی روسیه است تا رد پای خود را در این حملات مخفی کند.

امنیت‌سایبری

تروریست‌های داعشی شما را می‌بینند

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

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

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

کارشناسان BOC می‌گویند نگرانی اصلی آن‌ها این است که تروریست‌های داعشی از کنترل این دوربین‌ها برای مخفی‌کردن عملیات‌های مختلف خود استفاده کنند. البته نگرانی دیگر به استفاده از این دوربین‌های در حملات مختلف نظیر آنچه برای Dyn اتفاق افتاد مربوط می‌شود. «می‌دانیم که تروریست‌های داعشی پیش از انجام حمله به‌دقت محل موردنظر خود را بررسی می‌کنند، این امکان جدید می‌تواند در انجام حملات به‌شدت به آن‌ها کمک کند.»

در گزارش BOC آمده است: «انجام حملات به شکل ساده‌تر همان هدفی که به نظر می‌رسد گروهک تروریستی داعش می‌خواهد با استفاده از فناوری به آن دست یابد. در سال گذشته شاهد افزایش چشمگیر اطلاعات فنی و آموزشی در این گروهک بوده‌ایم. عملیات‌های این‌چنینی از سوی داعش برای گذراندن وقت بر روی اینترنت نیست؛ آن‌ها باهوش هستند. به همین دلیل، بیش از پیش اهمیت دارد که آژانس‌های جاسوسی از منابع برخط خود محافظت کنند. سازمان‌ها نیز باید اقدامات مختلف امنیتی را انجام دهند تا مانع از بهره‌برداری گروه‌های تروریستی از ابزارهای نظارتی همچون دوربین‌های امنیتی شوند.»

امنیت‌سایبری

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

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

در این بیانیه آمده است: «USIC اطمینان دارد که دولت روسیه سوءاستفاده‌های اخیر از رایانامه‌های افراد و سازمان‌های مختلف آمریکایی از جمله سازمان‌های سیاسی را مدیریت می‌کرده است. بررسی رایانامه‌های مورد نفوذ واقع‌شده و منتشرشده در وبگاه‌هایی مانند DCLeaks.com و ویکی‌لیکس شواهدی را مبنی بر شباهت این حملات با روش‌هایی که روسیه استفاده می‌کند، نشان داده است. این سرقت‌ها و نفوذها در نظر دارند در روند انتخابات آمریکا تداخل ایجاد کنند.»

دو هفته پیش، معاون رئیس‌جمهور آمریکا، جو بایدن طی یک مصاحبه با شبکه خبری NBC گفته بود: «پیامی درباره حملات مذکور به ولادمیر پوتین داده خواهد شد.» به گزارش NBC، سازمان CIAدر حال آماده‌سازی حمله‌ی سایبری تلافی‌جویانه است تا به مقابله با کرملین بپردازد. درحالی‌که متخصصان امنیتی، سیاست‌مداران و مقامات ارتش درباره نحوه پاسخ مناسب به مداخلات روسیه فکر می‌کنند، افسر ارشد سازمان اطلاعات ملی با استناد به اسناد فوق محرمانه می‌گوید ارتش سایبری ایالات متحده قبلاً به شبکه توزیع برق، شبکه ارتباطی و سامانه‌های فرمان روسی نفوذ کرده است.

روسیه، چین، آمریکا، آلمان و تقریباً تمام کشورها در حال تقویت توانایی‌های سایبری خود هستند. این روند تا جایی پیش رفته است که متخصصان امنیتی اصطلاح نظامی کردن فضای سایبری را برای آن استفاده کرده‌اند. این اصطلاح به معنای تلاش دولت‌ها به‌منظور دستیابی به‌نوعی سلطه در استفاده از بدافزارها و ابزارهای نفوذ علیه زیرساخت‌های حیاتی و سامانه‌های رایانه‌ای سایر کشورها است. مثال‌هایی همچون استاکس‌نت میزان تأثیر اسلحه‌های دیجیتال را در دنیای امروز نشان داده‌اند. اخیراً نفوذگران روسی متهم به راه‌اندازی پویش‌های خرابکارانه‌ای علیه دولت‌ها و شرکت‌های مختلف در نقاط مختلف شده بودند. البته که ارتش سایبری آمریکا نیز در همین جهت پیش خواهد رفت. اسناد منتشرشده توسط ادوارد اسنودن و مجله Der Spiegel فاش می‌سازد که سازمان اطلاعات آمریکا به دنبال نوعی سلطه در فضای سایبری است.

سازمان اطلاعات آمریکا می‌گوید: «به نظر نمی‌رسد نفوذگران روسی زیرساخت‌های حیاتی ملی را هدف قرار دهند، بلکه ممکن است با انتشار اسناد جعلی و یا توزیع اطلاعات غلط از طریق پویش‌های PSYops به انتخابات هفته آینده ریاست جمهوری آمریکا لطمه وارد کنند.»

جیمز لوئیس، متخصص سایبری در مرکز مطالعات راهبردی و بین‌المللی می‌گوید: «آمریکا مدت‌هاست به زیرساخت‌های رایانه‌ای دولت‌های رقیب خود ازجمله چین، روسیه، ایران و کره شمالی نفوذ می‌کند.»

گری براون، یکی از مقامات ارشد سازمان اطلاعات ملی آمریکا در این خصوص می‌گوید: «در صورت مواجهه با یک حمله سایبری شاخص باید سه اقدام انجام شود؛ اول این‌که در برابر آن از خود دفاع کنیم، دوم باید افکار عمومی را درباره آنچه رخ داده است آگاه سازیم، سوم باید به این حمله پاسخ مناسب داده شود.»

فصل چهارم

اخبار فنی

اخبار فنی

اصلاح ۹ آسیب‌پذیری فلش‌پلیر

ادوبی، دو هفته پس از ارائه‌ی یک وصله‌ی اضطراری برای آسیب‌پذیری روز-صفرم خود، اقدام به انتشار یک به‌روزرسانی امنیتی دیگر برای فلش‌پلیر نموده است.

این انتشار تازه منجر به اصلاح ۹ آسیب‌پذیری می‌شود، همه‌ی این شکاف‌ها سامانه را در معرض اجرای از راه دور کد قرار می‌دهند. ادوبی گفت که از هرگونه سوءاستفاده‌ی عمومی از این آسیب‌پذیری‌ها اطلاعی ندارد.

ادوبی خاطرنشان کرد که نسخه‌های رومیزی 23.0.0.205 و قبل از آن در بسترهای ویندوز و مک، همچنین گوگل کروم و مایکروسافت اج و اینترنت اکسپلورر ۱۱ در ویندوز ۱۰ و ویندوز ۸٫۱ تحت تأثیر این آسیب‌پذیری‌ها قرار دارند.

این به روزرسانی به شش آسیب‌پذیری استفاده پس از آزادسازی، و سه مورد شکاف سردرگمی در نوع رسیدگی کرده که همگی در طرح ابتکاری روز-صفرم ترندمیکرو کشف و برملا شده‌اند.

ادوبی گفت که این به‌روزرسانی از نوع برنامه‌ریزی شده بوده است. دو هفته پیش، یک وصله‌ی اضطراری منجر به اصلاح آسیب‌پذیری با شناسه‌ی CVE-2016-7855 شد، از این آسیب‌پذیری در حملات هدف‌مند محدود سوءاستفاده به عمل آمده بود. این روز-صفرم و جزئیات حمله‌ی مربوط به آن به‌طور خصوصی توسط محققان تیم تحلیل تهدید گوگل افشاء شد، این گروه به‌طور خصوصی به بیان جزئیات یک روز-صفرم هسته‌ی ویندوز پرداخت که با روز-صفرم فلش مورد استفاده در حملات در ارتباط بود.

اگرچه ادوبی این روز-صفرم فلش را در عرض یک هفته پس از مطلع‌شدن از وجودش رفع کرد، گوگل ویژگی‌های آن را مو به مو برملا کرد. سیاست افشاسازی گوگل به شرکت‌ها یک فرصت ۶۰ روزه می‌دهد تا آسیب‌پذیری‌های حیاتی را رفع کنند، یا کاربران را در جریان این رخداد و خطرهای احتمالی قرار داده و هرگونه اقدام لازم برای بهبود اوضاع را به آن‌ها گوشزد کنند.

این سیاست که در سال ۲۰۱۳ منتشر شد، شامل یک مهلت هفت‌روزه برای آسیب‌پذیری‌های حیاتی است که مورد سوءاستفاده واقع شده‌اند. انتظار می‌رود که مایکروسافت این روز-صفرم را در خلال وصله‌ی سه‌شنبه‌ی خود اصلاح نماید. ادوبی همچنین نرم‌افزار کنفرانس تحت وب Connect خود را هم ترمیم نمود.

این به‌روزرسانی یک آسیب‌پذیری اعتبارسنجی ورودی را در ماژول ثبت وقایع از میان برداشته که باعث انجام حملات تزریق کد می‌شد. ادوبی می‌گوید که نسخه‌ی 9.5.6 و قبل از آن از این شکاف رنج می‌برند. ادوبی به کاربران توصیه می‌کند که هرچه سریع‌تر به‌روزرسانی به نسخه‌ی 9.5.7 را در برنامه‌ی کار خود قرار دهند.

اخبار فنی

اصلاح آسیب‌پذیری اجرای کد در GitLab

این هفته توسعه‌دهندگان GitLab یک آسیب‌پذیری حیاتی را در این نرم‌افزار متن‌باز مدیریت مخزن اصلاح کردند؛ این آسیب‌پذیری منجر به اجرای دستور شده و به یک کاربر احراز هویت شده اجازه می‌داد به پرونده‌ها، توکن‌ها یا اسرار نرم‌افزارهای حساس دسترسی پیدا کند. یکی از مؤسسان HackerOne به نام جوبرت آبما هفته‌ی گذشته این آسیب‌پذیری را کشف کرد و طی برنامه‌ی کشف خطای گیت‌لب آن را گزارش نمود. گیت‌لب با انتشار نسخه‌ی 8.13.3 در ساعات پایانی روز چهارشنبه به این شکاف (با شناسه‌ی CVE-2016-9086) رسیدگی کرد. این مشکل، یعنی آسیب‌پذیری خواندن پرونده‌ی دلخواه، در قابلیت ورود/خروج گیت‌لب وجود دارد، و در واقع ترکیبی از رفع خطا، رفتار تابع جاوااسکریپت JSON.parse، و نیز توانایی درج پیوندهای نمادین در ورودی گیت‌لب می‌باشد. پیوندهای نمادین، که تحت عنوان پیوندهای نمادی هم از آن‌ها یاد می‌شود، کلیدهای میان‌بری هستند که به پرونده‌ها، پوشه‌ها، یا دایرکتوری‌های دیگر اشاره دارند. آبما متوجه شد که به خاطر این مشکلات توانسته به محتوای یک پرونده که در یک پیام خطا رمزگشایی می‌شود دسترسی پیدا نماید.

در ادامه نفوذگر می‌تواند از این شکاف برای خواندن اسرار یک پروژه‌ی GitLab Rails، توکن‌های پوسته که برای احراز هویت کاربران گیت‌لب استفاده می‌شوند و حتی اجرای از راه دور کد سوءاستفاده نماید.

با وجود این مسئله، پروژه‌ی ریل گیت‌لب را هم می‌توان خواند. این موضوع به خاطر یک اجرای از راه دور کد امکان‌پذیر است، چون کوکی‌ها را می‌توان مرتب‌سازی کرد و مجدداً امضاء نمود. به نظر می‌رسد که حتی امکان دستیابی به توکن‌های پوسته‌ی داخلی گیت‌لب هم امکان‌پذیر باشد، که در نهایت موجب دسترسی به همه‌ی مخزن‌ها می‌شود. قابلیت ورود/خروج، که گیت‌لب به نسخه‌ی 8.9 اضافه کرده است، به تازگی برای همه‌ی کاربران در نسخه‌ی 8.13 اضافه شده است.

گیت‌لب در وهله‌ی نخست کاربران را از ارائه‌ی وصله‌ی لازم در روز دوشنبه و از طریق خبرنامه‌ی امنیتی خود آگاه کرد. گیت‌لب که آسیب‌پذیری‌های مشابه در 8.12.8، 8.11.10 و 8.10.13 را در نسخه‌ی CE و EE خود از میان برداشته است، تمام کاربرانی که نسخه‌ی آسیب‌پذیر را اجرا می‌کنند تشویق می‌کند تا هرچه سریع‌تر به‌روزرسانی و ارتقای لازم را صورت دهند.

اخبار فنی

شرکت سیسکو آسیب‌پذیری‌های موجود در مسیریاب‌های سری ۹۰۰ را برطرف می‌کند

شرکت سیسکو دو مورد آسیب‌پذیری با درجه شدت بالا را برطرف کرده است که بر روی محصولاتی همچون مسیریاب‌های Series 900، کارگزار Prime Home و بستر مدیریت شبکه ابری اثرگذار بوده‌اند. این شرکت با انتشار دو مشاوره امنیتی اشکالات مذکور را به مشتریان گزارش داده است. یکی از این مشاوره‌های منتشرشده به ارائه‌دهندگان خدماتی که از مسیریاب‌های ASR 900 Series استفاده می‌کنند درباره یک آسیب‌پذیری هشدار می‌دهد که با CVE-2016-6441 شناسایی می‌شود. آسیب‌پذیری مذکور در کد زبان تراکنش شماره یک (TL1) مسیریاب کشف شده است. این آسیب‌پذیری می‌تواند توسط یک مهاجم از راه دور به‌منظور اجرا کد مخرب مورد بهره‌برداری قرار گیرد.

«این آسیب‌پذیری به این دلیل وجود دارد که نرم‌افزار تحت تأثیر، بررسی‌های کامل را بر روی داده‌های ورودی انجام نمی‌دهد. یک مهاجم می‌تواند با ارسال یک درخواست مخرب به درگاه TL1 از این آسیب‌پذیری بهره‌برداری کند. این بهره‌برداری به مهاجم اجازه می‌دهد کد دلخواه خود را اجرا کرده و کنترل کامل سامانه را به دست گیرد.»

شرکت سیسکو به‌روزرسانی‌های لازم را برای برطرف‌سازی این آسیب‌پذیری در اختیار عموم قرار داده است.

اشکال امنیتی دوم یک آسیب‌پذیری عبور از احراز هویت است که با CVE-2016-6452 شناسایی شده و در واسط کاربری گرافیکی تحت وب محصول Prime Home از شرکت سیسکو کشف شده است. این آسیب‌پذیری می‌تواند توسط مهاجم از راه دور و به‌منظور دور زدن فرآیند احراز هویت مورد بهره‌برداری قرار گیرد. مهاجم می‌تواند درخواست دستکاری شده HTTP به یک URL خاص را ارسال کند، بدین‌ترتیب یک شناسه جلسه معتبر برای کاربر دلخواه ایجاد می‌شود. «مهاجم با بهره‌برداری از این آسیب‌پذیری می‌تواند اختیارات مدیریتی را به دست آورد. این آسیب‌پذیری به دلیل خطای پردازش در کنترل دسترسی مبتنی بر نقش (URL RBAC) ها رخ می‌دهد. مهاجم می‌تواند درخواست دستکاری شده HTTP را ارسال کند، بدین‌ترتیب یک شناسه جلسه معتبر برای کاربر دلخواه ایجاد می‌شود. بنابراین مهاجم می‌تواند هر کاری را که کاربر مذکور اجازه انجام آن را دارد در Prime Home انجام دهد. نقش کاربری مذکور می‌تواند شامل سطح اختیارات مدیر سامانه نیز باشد.»

اخبار فنی

بهره‌برداری از سامانه‌های PLC از طریق حملات کنترل پین

محققان امنیتی در همایش کلاه‌سیاه‌های اروپا ۲۰۱۶، روش جدیدی از حمله را نشان داده‌اند که بدون اینکه شناسایی شود می‌تواند برای نفوذ به کنترلرهای منطقی برنامه‌پذیر (PLC) به کار رود.

کنترلرهای منطقی برنامه‌پذیر اجزای ضروری برای نظارت و کنترل فرآیندهای فیزیکی در محیط‌های صنعتی هستند.

در ماه سپتامبر، محقق امنیتی علی عباسی، دانشجوی دکتری دانشگاه Twente در هلند به همراه محقق امنیتی مستقل، مجید هاشمی، اعلام کردند توانسته‌اند یک روت‌کیت PLC غیرقابلشناسایی بسازند. آن‌ها هفته گذشته روت‌کیت خود را در همایش کلاه‌سیاه‌های اروپا در لندن ارائه کردند. آن‌ها همچنین نوعی از حمله PLC را ارائه کردند که از کد پوسته استفاده می‌کند. آن‌ها می‌گویند روش حمله روت‌کیت آن‌ها مانند سایر بدافزارها کد منطقی PLC را هدف قرار نمی‌دهد و همین امر موجب می‌شود شناسایی این حمله سخت باشد. «فعالیت روت‌کیت PLC حتی برای سامانه‌هایی که بر مصرف توان کنترلرهای منطقی برنامه‌پذیر نظارت می‌کنند نیز قابل شناسایی نیست.»

سامانه‌های PLC سیگنال‌های ورودی خود را از حسگرهایی می‌گیرند که برای نظارت بر فرآیندهای صنعتی استفاده می‌شوند. بدافزار مذکور در ارتباط بین منطق و زمان اجرای PLC با ورودی/خروجی‌های تداخل ایجاد می‌کند. این بدافزار در حافظه پویای جز صنعتی قرار گرفته، ورودی/خروجی و فرآیند PLC را دستکاری می‌کند. واضح است که دستکاری سیگنال‌های ورودی/خروجی می‌تواند بدون شناسایی موجب تداخل در فرآیند صنعتی شود، این همان کاری است که روت‌کیت PLC مذکور انجام می‌دهد.

این دو متخصص در مقاله خود می‌گویند: «در این مقاله علاوه بر توانایی‌های حمله مذکور که در نتیجه حمله کنترل پین حاصل می‌شود، نیازمندی‌های لازم برای اجرای این حمله نیز نشان داده شده است. توانایی‌های این حمله شامل مسدودسازی ارتباطات با دستگاه‌های جانبی، صدمه زدن به دستگاه‌های جانبی و دستکاری مقادیری می‌شود که توسط فرآیند قانونی خوانده شده و یا نوشته می‌شوند. در این مقاله نشان می‌دهیم چگونه می‌توان از کنترل پین هم در شرایطی که مهاجم دسترسی سطح هسته و یا ریشه دارد و هم در شرایطی که دسترسی‌های مذکور را ندارد بهره‌برداری نمود.»

عباسی و هاشمی دو روش جداگانه حمله کنترل پین را ابداع کرده‌اند. در روش اول، مهاجم از یک کد مخرب برای تغییر تنظیمات پین استفاده می‌کند تا پین‌های ورودی را به خروجی (و بالعکس) تغییر دهد. در سناریوی

دوم حمله، مهاجم با تغییر عملکرد همان پین از ویژگی تسهیم (multiplexing) سوءاستفاده می‌کند. در این روش کنترلر منطقی برنامه‌پذیر نمی‌تواند کار خود را به درستی انجام دهد.

نکته قابل توجه این‌که هر دو روش تغییر پین و تسهیم پین هیچ‌گونه هشداری را فعال نمی‌کنند. به همین دلیل هر دو نوع حمله می‌توانند فرآیندهای شناسایی نفوذ همچون Autoscopy Jr را در سامانه‌های کنترل توکار دور بزنند.

این دو محقق می‌گویند می‌توان روت‌کیتی نوشت که حمله مذکور را انجام دهد، اما بدین‌ترتیب مهاجم نیازمند دسترسی ریشه به سامانه PLC خواهد بود. در سناریوی دوم اگر مهاجم همان دسترسی زمان اجرای PLC را داشته باشد می‌تواند در قالب آسیب‌پذیری RCE بهره‌برداری مذکور را انجام دهد.

هر دوی حملات گفته شده می‌توانند برای ایجاد شرایط منع سرویس و کنترل فرآیند فیزیکی متصل به PLC استفاده شوند. این دو محقق خاطر نشان کرده‌اند که حمله بدون دسترسی ریشه کاراتر بوده اما دقت کمتری دارد. آن‌ها می‌گویند بیشتر کنترلرهای منطقی برنامه‌پذیر موجود در بازار در برابر حملات آن‌ها آسیب‌پذیر هستند؛ به همین دلیل شرکت‌های سازنده مختلف را درباره این حملات آگاه کرده‌اند. مقاله منتشر شده توسط این محققان همچنین روش‌های مقابله با این نوع حملات را بیان کرده است.

اخبار فنی

۵ نکته‌ای که باید درباره شبکه‌های خصوصی مجازی بدانید

یک شبکه خصوصی مجازی یک تونل امن بین یک یا چند رایانه بر روی اینترنت است. این شبکه به رایانه‌های مذکور اجازه می‌دهد اگر بر روی یک شبکه محلی باشند به یکدیگر دسترسی داشته باشند. در گذشته، VPN ها توسط شرکت‌های مختلف و برای برقراری ارتباط امن از راه دور بین شعب مختلف استفاده می‌شد. کاربری دیگر نیز توسط کارمندان برای اتصال به شبکه محل کار بود؛ اما امروزه این شبکه‌های خصوصی مجازی خدمات مهمی برای مشتریان نیز محسوب می‌شوند، چرا که در زمان اتصال به شبکه‌های بی‌سیم عمومی از آن‌ها در برابر حملات محافظت می‌کنند.

VPN ها راهکاری مناسب برای تأمین امنیت و حریم خصوصی هستند

شبکه‌های بی‌سیم عمومی خطری جدی برای کاربران محسوب می‌شوند، چرا که مهاجمان در این شبکه‌ها می‌توانند با به‌کارگیری روش‌های مختلف به استراق سمع ترافیک کاربران پرداخته و یا حساب‌های کاربری آنان را بر روی وبگاه‌هایی که از پروتکل امنیتی HTTPS استفاده نمی‌کنند به سرقت ببرند. به‌علاوه، برخی اپراتورهای شبکه وای‌فای آگاهانه تبلیغات را به ترافیک وب تزریق می‌کنند؛ این تبلیغات می‌توانند منجر به ردیابی ناخواسته شوند. در برخی کشورها، دولت‌ها کاربرانی که به وبگاه‌های خاصی سر می‌زنند از نظر سیاسی تحت پیگرد قرار می‌دهند. این‌گونه عملیات آزادی بیان را تهدید می‌کند. با استفاده از ارتباط VPN همه ترافیک شما به‌طور امنی از طریق کارگزاری که در جای دیگری از دنیا قرار دارد مسیریابی می‌شود. این فرآیند از رایانه شما در برابر ردیابی‌های محلی و نفوذهای احتمالی جلوگیری کرده و آدرس IP شما را از وبگاه‌ها و خدماتی که دسترسی داشته‌اید مخفی می‌کند.

همه VPNها یکسان نیستند

انواع فناوری‌های VPN با توانایی‌های رمزنگاری متفاوت وجود دارند. برای مثال، پروتکل PPTP سریع بوده اما از سایر پروتکل‌هایی همچون IPSec و یا OpenVPN که از SSL/TLS استفاده می‌کنند به لحاظ امنیتی ضعیف‌تر است. به‌علاوه، در ارتباطات مبتنی بر TLS نوع الگوریتم رمزنگاری و طول کلید نیز مهم است.

درحالی‌که OpenVPN از ترکیبات مختلف رمز، پروتکل‌های تبادل کلید و الگوریتم‌های درهم‌سازی پشتیبانی می‌کند، رایج‌ترین پیاده‌سازی توسط ارائه‌دهندگان خدمات VPN برای ارتباطات OpenVPN رمزنگاری AES با تبادل کلید RSA و امضای SHA است. تنظیمات توصیه شده شامل رمزنگاری AES-256 با یک کلید RSA است که حداقل ۲۰۴۸ بیت طول داشته و از تابع درهم‌سازی SHA-2 به‌جای SHA-1 استفاده می‌کند.

نکته شایان ذکر این است که VPNها همراه با سربار هستند؛ هر چه رمزنگاری قوی‌تر باشد، تأثیر منفی بر روی سرعت ارتباط نیز بیشتر خواهد بود. انتخاب فناوری VPN و قدرت رمزنگاری به نوع داده مورد استفاده بستگی دارد.

نیازهای امنیتی کاربران عادی با شرکت‌ها متفاوت است. کاربران بیشتر می‌خواهند در برابر حملات استراق سمع احتمالی از خود محافظت کنند حال آن‌که در بیشتر موارد شرکت‌ها امنیت بیشتری را طلب می‌کنند.

VPN می‌تواند دیواره‌آتش و مسدودسازی‌های مبتنی بر موقعیت جغرافیایی را دور بزند

کاربران همچنین از VPN ها استفاده می‌کنند تا به محتواهای برخطی که در موقعیت مکانی آن‌ها قابل دسترسی نیست، دست یابند؛ البته این مهم به این بستگی دارد که چقدر مدیران محتوای مذکور بخواهند محدودیت‌ها را اعمال کنند. ارائه‌دهندگان خدمات VPN معمولاً کارگزارهایی را در کشورهای مختلف راه‌اندازی می‌کنند تا برای کاربران این امکان را فراهم سازند به‌راحتی بین آن‌ها سوئیچ کنند. برای مثال کاربران ممکن است برای دسترسی به محتوای BBC که در مکانی مسدود است از کارگزارهای انگلیسی استفاده کنند.

کاربران کشورهایی همچون چین و یا ترکیه که به دلایل سیاسی دولت به‌طور مرتب دسترسی به وبگاه‌هایی را مسدود می‌سازد معمولاً از VPN برای دور زدن چنین محدودیت‌هایی استفاده می‌کنند.

VPN های رایگان در برابر غیر رایگان

درحالی‌که شرکت‌های مختلف VPN های خود را با استفاده از ابزارهای شبکه‌ای خاص راه‌اندازی می‌کنند، کاربران معمولاً بازه وسیعی از انتخاب خدمات VPN رایگان و یا تجاری دارند. خدمات VPN رایگان معمولاً حاوی تبلیغات بوده و کاربر انتخاب‌های کمتری برای کارگزارها دارد. به‌علاوه سرعت اتصال در این نوع معمولاً پایین‌تر است چرا که کارگزارهای این خدمات معمولاً با درخواست‌های بیشتری مواجه هستند. البته برای یک کاربر عادی معمولاً همین نوع VPN کفایت می‌کند.

اشکال دیگر کارگزارهای VPN رایگان این است که احتمال مسدودشدن آدرس‌های IP آن‌ها بر روی وبگاه‌های مختلف بیشتر است: خدمات VPN رایگان به فراوانی توسط نفوذگران، ارسال‌کنندگان هرزنامه و کاربران مخرب استفاده می‌شوند.

خدمات VPN تجاری بر مبنای مدل‌های اشتراکی تعریف شده و سرعت بارگیری و یا محدودیت داده متفاوت دارند. برخی از آن‌ها می‌گویند هیچ‌گونه گزارشی را از فعالیت کاربران نگهداری نمی‌کنند تا بتوان با استفاده از آن‌ها کاربران را شناسایی کرد.

برخی از شرکت‌های ضدویروس هم خدمات VPN ارائه می‌دهند و این خدمات جایی بین نوع رایگان و نوع تجاری قرار می‌گیرند. در این موارد کاربران اگر از شرکت مذکور گواهی استفاده از ضدویروس داشته باشند از امکانات بهتری برای VPN می‌توانند استفاده کنند. به‌علاوه این نوع VPN ها تنظیمات امنیتی قابل قبولی دارند و نیازی نیست کاربران درباره تنظیم آن‌ها نگرانی داشته باشند.

VPN خود را بسازید

درنهایت این گزینه هم وجود دارد که کارگزار VPN خود را به‌طور خانگی راه‌اندازی کنید. البته راه بهتری هم وجود دارد که خدمات مذکور در معرض اینترنت قرار نگیرند. در ابتدای ماه جاری صدها هزار دستگاه اینترنت اشیاء که در معرض اینترنت بودند توسط نفوذگران مورد سوءاستفاده قرار گرفته و در حملات منع سرویس توزیع‌شده بهره‌برداری شدند.

قانون کلی این است که هر چه درگاه‌های کمتری بر روی مسیریاب باز باشند بهتر است. شما باید UPnP را غیرفعال کنید، بدین‌ترتیب برای مثال دوربین IP شما از طریق اینترنت در معرض دسترسی همگان نخواهد بود. امروزه برخی مسیریاب‌ها عملکرد VPN را در خود دارند بنابراین لازم نیست یک کارگزار VPN مجزا را در شبکه خود راه‌اندازی کنید. اگر مسیریاب شما این کار را انجام نمی‌دهد می‌توانید از یک رایانه کوچک مانند Raspberry Pi برای این کار استفاده کنید.

اخبار فنی

بازنشانی کلمات‌عبور پورتال Careers از سوی سیسکو

هفته گذشته شرکت سیسکو اطلاع داد قصد دارد پس از کشف یک آسیب‌پذیری در پورتال مشاغل (Careers) عملیات بازنشانی کلمه‌عبور را بر روی حساب‌های کاربری این وبگاه انجام دهد.

این غول شبکه گفته است این اقدام را به‌منظور حفظ امنیت حساب‌های کاربری انجام می‌دهد. سیسکو می‌گوید در اثر این اشکال امنیتی تعداد محدودی از اطلاعات مرتبط با درخواست مشاغل در معرض خطر قرار گرفته‌اند. «ما معتقدیم به‌جز محققی که آسیب‌پذیری مذکور را کشف کرده است فرد دیگری به این اطلاعات دسترسی پیدا نکرده است.»

سیسکو می‌گوید اشکال مذکور در اثر تنظیمات امنیتی اشتباهی رخ داده است که یک شرکت سوم شخص مسئولیت آن را بر عهده داشته است. به‌محض این‌که سیسکو از این اشکال آگاه شده است، تنظیمات مربوطه را اصلاح کرده و درخواست بازنشانی حساب‌کاربری را بر روی وبگاه قرار داده است.

آسیب‌پذیری مذکور توسط یک محقق امنیتی مستقل کشف شده بود. بررسی‌های این محقق نشان داده است که تنظیمات اشتباه دو مرتبه رخ داده‌اند: از آگوست ۲۰۱۵ تا سپتامبر ۲۰۱۵ و از جولای ۲۰۱۶ تا آگوست ۲۰۱۶.

در هشدار رخنه منتشر شده از سوی شرکت سیسکو آمده است که داده‌های در معرض خطر شامل نام کاربران، آدرس، رایانامه، شماره تلفن، نام‌کاربری و کلمه‌عبور، پاسخ به سؤالات امنیتی، پروفایل آموزشی و حرفه‌ای، رزومه افراد و سایر اطلاعات اختیاری از جمله جنسیت و نژاد بوده است.

شرکت سیسکو می‌گوید معتقد است تنها محققی که اشکال مذکور را کشف کرده است به داده‌ها دسترسی پیدا کرده، اما این شرکت نگفته است که یک نمونه اتصال غیرعادی به کارگزار موجب شده است آن‌ها اقدامات پیشگیرانه را انجام دهند.

در تاریخ ۲ نوامبر این شرکت تصمیم گرفت به کاربران خود هشدار دهد به‌محض این‌که به وبگاه Professional Career وارد شدند با کلیک بر روی گزینه «فراموشی کلمه‌عبور» کلمه‌عبور حساب خود را تغییر دهند. به‌علاوه این شرکت تصمیم گرفت دسترسی به وبگاه را از طریق سؤال امنیتی غیرفعال کند.

به گفته سیسکو کاربرانی که رایانامه هشدار را برای تغییر کلمه‌عبور دریافت کرده‌اند می‌بایست کلمات‌عبور خود را در سایر وبگاه‌ها نیز تغییر دهند، به‌خصوص اگر از همان کلمه‌عبور در سایر وبگاه‌ها استفاده کرده‌اند.

سیسکو می‌گوید به بررسی‌های خود درباره این آسیب‌پذیری و سوءاستفاده‌های احتمالی ادامه می‌دهد؛ به‌علاوه گام‌هایی را در جهت پیشگیری از شرایط مشابه در آینده انجام خواهد داد.

اخبار فنی

کشف دامنه‌های مخرب و جلوگیری از حملات فیشینگ با ابزار PhishEye

داده که دامنه‌های بالقوه‌ی خطرناک را شناسایی می‌کند.

این راه‌حل که PhishEye نام دارد فرآیند تشخیص دامنه‌های شبیه به هم را خودکار می‌سازد. از این طریق دامنه‌هایی که توسط مهاجمان برای جعل نام دامنه‌های نام‌های تجاری، محصولات و شرکت‌ها استفاده می‌شود را می‌توان شناسایی کرد. این ابزار می‌تواند به گروه‌های امنیتی در برطرف کردن تهدیدات مبتنی بر نام دامنه کمک کند و در آینده به‌طور چشمگیری حملات فیشینگ را کاهش دهد.

در حملات فیشینگ، نام دامنه‌ها به شکلی جعل می‌شود که کاربرِ قربانی در نگاه اول متوجه غیرقانونی بودن آن نمی‌شود. PhishEye ابزاری است که سازمان‌ها برای کشف و شناسایی دامنه‌های مخرب می‌توانند از آن استفاده کنند.

این ابزار از الگوریتم تطبیق زیررشته‌ای و تایپی که ترکیبی از موتور اعتبار دامنه مخصوص DomainTools است استفاده می‌کند تا دامنه‌های مخرب را کشف کند. این ابزار تلاش می‌کند به محض ثبت شدن این دامنه‌ها و شناسایی آن به کاربر هشدار دهد.

دامنه‌هایی که توسط این ابزار کشف شدند، برای جلوگیری از حملات فیشینگ در آینده می‌توانند به مسدودکننده‌ی هرزنامه، دیواره آتش و سایر سازوکارهای امنیتی وارد شوند. کاربران همچنین می‌توانند دامنه‌های کشف‌شده را برای بررسی و انتساب دقیق‌تر به DomainTools Iris ارسال کنند.

در برخی موارد مهاجمان با ایجاد دامنه‌های جعلی به نام و شهرت یک شرکت آسیب می‌رسانند و یا با ثبت دامنه‌هایی سعی در نظارت بر عملیات یک سازمان داشته یا فعالیت‌های قانونی علیه آن‌ها انجام می‌دهد. این ابزار برای تشخیص چنین دامنه‌هایی مفید خواهد بود. مجرمان در فضای مجازی می‌توانند آدرس رایانامه‌ها را جعل کرده و در رایانامه‌ی خود پیوندی فریبنده قرار دهند تا قربانی روی آن کلیک کند و بدین ترتیب سازمان‌ها هر ساله به‌طور میانگین میلیون‌ها دلار ضرر و زیان را متحمل می‌شوند. گروه کاری ضد-فیشینگ (APWG) گزارش داده است که تعداد وب‌گاه‌های منحصربفرد فیشینگ در سه‌ماهه‌ی دوم سال 2016 به میزان 61 درصد افزایش یافته و نسبت به سه‌ماهه‌ی چهارم سال 2015 سه برابر شده است.

اخبار فنی

گوگل برای آسیب‌پذیری گاو کثیف وصله‌ی تکمیلی منتشر کرد

روز دوشنبه بولتن امنیتی اندروید برای ماه نوامبر منتشر شد که در آن به‌طور کلی 85 آسیب‌پذیری برطرف شده بود که 15 مورد از این آسیب‌پذیری‌ها جدی بود. اما آشکارا آسیب‌پذیری شرایط رقابتی لینوکس که با نام گاو کثیف هم شناخته می‌شد (Copy-on-Write) و اندروید را نیز تحت تاثیر قرار می‌داد، همچنان وجود دارد و برطرف نشده است.

در حالی‌که گوگل برای آسیب‌پذیری گاو کثیف با شناسه‌ی CVE-2016-5195 وصله‌ای ارائه نکرده است، اما برای گوشی‌های نکسوس و پیکسل به‌روزرسانی‌های تکمیلی ثابت‌افزار را منتشر کرده است. براساس گزارش محققان امنیتی، شرکت سامسونگ برای آسیب‌پذیری گاو کثیف وصله‌ای ارائه کرده است (SMR-NOV-2016) در حالی‌که سایر شرکت‌های تولیدکننده‌ی گوشی هنوز این کار را نکرده‌اند.

به گفته‌ی گوگل، وصله برای آسیب‌پذیری گاو کثیف به‌طور رسمی توسط دیگر سازندگان گوشی اندروید در ماه دسامبر در بولتن امنیتی اندروید معرفی خواهد شد.

در آغاز بررسی بولتن امنیتی این ماه بهتر است اشاره کنیم که گوگل دسته‌بندی جدیدی را برای وصله‌های ارائه‌شده در نظر گرفته است: جزئی، کامل، تکمیلی. گوگل می‌گوید نام‌گذاری مربوط به سطوح جزئی و کامل مشخص است که چیست و وصله‌های سطح تکمیلی برای شناسایی دستگاه‌هایی ارائه شده که این مشکل قبلاً در آن‌ها و پیش از ارائه‌ی وصله‌ها برطرف شده است.

آسیب‌پذیر گاو کثیف تنها وصله در بولتن امنیتی اندوید با سطح تکمیلی بود. گوگل 12 آسیب‌پذیری جدی ارتقاء امتیازات را در این بولتن وصله کرده که 9 مورد از این آسیب‌پذیری‌ها در هسته‌های زیرسامانه‌ی اندوید وجود داشتند. برخی از این اشکالات به گفته‌ی گوگل مربوط به راه‌انداز SCSI اندروید (CVE-2015-8962)، راه‌انداز رسانه (CVE-2016-6737) با نام ION هستند.

آسیب‌پذیری ION با نام (AKA Drammer) ماه گذشته توسط آزمایشگاه VUSec گزارش شد. این اشکال مربوط به سخت‌افزار اندروید و ماژول‌های حافظه‌ی DRAM بود که به مهاجم اجازه‌ی دسترسی ریشه بر روی سامانه‌ی هدف را می‌داد. این آسیب‌پذیری می‌تواند بر روی گوشی‌های مختلفی از جمله نکسوس، سامسونگ، الجی و موتورولا دسترسی ریشه را به مهاجم بدهد.

به گفته‌ی گوگل مسئله‌ی مشکل‌ساز وجود 7 آسیب‌پذیری ارتقاء امتیاز در راه‌انداز GPU انویدیا است. گوگل در بولتن امنیتی اندروید نوشت: «آسیب‌پذیری ارتقاء امتیاز در راه‌انداز GPU انویدیا می‌تواند یک برنامه‌ی مخرب محلی را قادر سازد تا در داخل هسته کد دلخواه را اجرا کند. با توجه به اینکه احتمال آلوده شدن دستگاه محلی وجود دارد و باید برای تعمیر دستگاه، سامانه عامل ری‌فلش

شـود، بـه ایـن آسـیب‌پذیری درجـه‌ی جـدی اختصـاص داده شـده اسـت.»

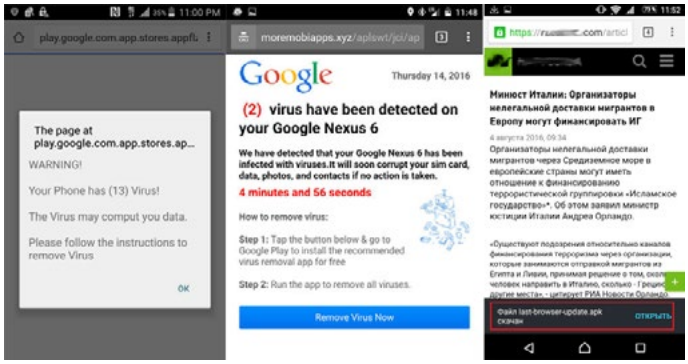
گـوگل همچنیـن 5 آسـیب‌پذیری جـدی اجـرای کـد از راه دور را وصلـه کـرده اسـت کـه مربـوط بـه مؤلفه‌هـای دسـتگاه اندرویـد همچـون مؤلفـه‌ی کارگـزار رسـانه (CVE-2016-6699) هسـتند. ایـن آسـیب‌پذیری توسـط محققـی از شرکـت علی‌بابـا کشـف شـد کـه مهاجـم را قـادر می‌سـازد بـا اسـتفاده از یـک پرونـده‌ی رسـانه‌ی جعلـی در داخـل مؤلفـه‌ی کارگـزار رسـانه باعـث خرابـی حافظـه شـده و بتوانـد کـدی را از راه دور اجـرا کنـد.

3 وصلـه‌ی مهـم و جـدی نیـز بـرای مؤلفـه‌ی Qualcomm گـزارش شـده اسـت. ایـن وصله‌هـا درسـت یـک مـاه پـس از ایـن ارائـه می‌شـود کـه گـوگل در وصلـه‌ی قبلـی خـود آسـیب‌پذیری سـطح بـالای QuadRooter را برطـرف کـرده بـود. ایـن آسـیب‌پذیری 900 میلیـون گوشـی اندرویـدی را در معـرض خطـر قـرار مـی‌داد. خطر جدیـدی کـه در Qualcomm وجـود دارد بـه گفتـه‌ی گـوگل مربـوط بـه راه‌انـداز crypto در ایـن مؤلفـه (CVE-2016-6725) و یـک آسـیب‌پذیری ارتقـاء امتیـاز در بوت‌لـودر Qualcomm بـا شناسـه‌ی CVE-2016-6729 اسـت.

گـوگل در خصـوص ایـن بولـتن امنیتـی گفتـه اسـت: «مـا هیـچ گزارشـی در خصـوص بهره‌بـرداری از دسـتگاه‌های مشـتریانمان یـا آسـیب‌پذیری‌هایی کـه اخیـراً گـزارش شـده، دریافـت نکردیـم.»

اخبار فنی

نفوذ به ۳۰۰ هزار دستگاه اندرویدی به دلیل آسیب‌پذیری در مرورگر کروم



یک آسیب‌پذیری که در مرورگر کروم اندروید وجود دارد، به مهاجم اجازه‌ی بارگیری تروجان بانکی در قالب برنامه‌های کاربردی را بدون تایید قربانی می‌دهد.

ممکن است شما نیز با یک تبلیغات pop-up در تلفن همراه خود مواجه شده باشید که به شما می‌گوید دستگاه شما آلوده به ویروس شده است و به شما توصیه می‌کند هرچه سریع‌تر یک برنامه‌ی امنیتی را نصب کنید. این صفحات وب تبلیغاتی مخرب، یک پرونده‌ی نصب برنامه‌ی اندورید (.apk) را بدون نیاز به تایید شما بارگیری می‌کند. مهاجم شما را مجبور خواهد کرد تا برای نصب این برنامه از فروشگاهی بجز فروشگاه خود گوگل، تنظیمات دستگاه خود را تغییر دهید. این برنامه در واقع یک تروجان بانکی است.

دو محقق کسپرسکی اولین بار این پویش تبلیغاتیِ مخرب را بر روی وب‌گاه‌های خبری روسیه و سایر وب‌گاه‌های معروف کشف کردند. از ماه آگوست تا به الان این تروجان نزدیک به 318 هزار دستگاه اندرویدی را در سراسر دنیا آلوده کرده است. این توزیع با استفاده از سرویس تبلیغاتی گوگل با نام AdSense و سوءاستفاده از آن برای گسترش این تروجان بانکی با نام Svpeng انجام شده است.

این دو محقق در پست وبلاگ خود توضیح دادند: «وقتی یک پرونده‌ی APK به تکه‌هایی شکسته می‌شود و قابلیت خود را با دست به دست شدن توسط کلاس Blob() حفظ می‌کند، بررسی بر روی محتوایی که ذخیره می‌شود، وجود نخواهد داشت و مرورگر این پرونده‌ی APK را بدون هشدار به کاربر ذخیره می‌کند.»

گوگل وجود این مسئله را تایید کرده است و در حال حاضر تبلیغات مخرب مسدود شده و برای وصله‌ی این آسیب‌پذیری برنامه‌ریزی شده است. هرچند هنوز مشخص نیست نسخه‌ی بعدی مرورگر کروم چه زمانی منتشر شود. به هرحال اگر گوگل بخواهد چرخه‌ی 6 ماهه‌ی انتشار کروم را ادامه دهد، انتظار می‌رود در به‌روزرسانی 3 دسامبر 2016 این آسیب‌پذیری وصله شود. با این حال حتی اگر گوگل در به‌روزرسانی بعدی نرم‌افزار خود این آسیب‌پذیری را وصله کند، مهاجمان هنوز برگ برنده‌ی دیگری دارند و می‌توانند با بهره‌برداری از این آسیب‌پذیری بر روی وب‌گاه‌های معروف، کاربران را به بارگیری این برنامه‌های مخرب وادار کنند.

به‌طور مثال نقص XSS که اخیراً بر روی وب‌گاه واتس‌اپ توسط محقق امنیتی هندی کشف شد، به مهاجم این امکان را می‌دهد تا کاربر را به بارگیری برنامه‌ی بدافزار مجبور کند.

بنابراین تنها راه‌کار مناسبی که برای جلوگیری از این مشکلات به ذهن می‌رسد این است که کاربران برنامه‌ها را تنها از فروشگاه نرم‌افزاری گوگل بارگیری کنند و به هیچ‌وجه تنظیمات تلفن همراه خود را برای بارگیری

برنامه‌ها از فروشگاه شخص ثالث تغییر ندهند. همچنین به کاربران توصیه می‌شود قبل از بارگیری برنامه از منابع غیرقابل اعتماد و از طریق پیوندهای مشکوک بیشتر فکر کنند.

اخبار فنی

مایکروسافت ۶۸ آسیب‌پذیری را وصله کرد

مایکروسافت 68 آسیب‌پذیری را در ویندوز، آفیس، اج، اینترنت اکسپلورر و SQL Server وصله کرده است. 2 مورد از این آسیب‌پذیری‌ها توسط مهاجمان مورد بهره‌برداری قرار گرفته و 3 مورد نیز به‌طور عمومی افشاء شده بود. این وصله‌ها در قالب 14 بولتن ارائه شده است. یکی از این بولتن‌ها به ادوبی فلش پلیر تخصیص داده شده که از طریق به‌روزرسانی ویندوز 10 و ویندوز 8.1 به‌روزرسانی شده است. 6 مورد از این بولتن‌ها درجه‌ی «جدی» و 8 مورد درجه‌ی «مهم» دریافت کرده‌اند.

مدیران سامانه باید وصله‌های ویندوز در بولتن MS16-135 را در اولویت قرار دهند زیرا این بولتن به آسیب‌پذیری‌های روز-صفرم که توسط مهاجمان گروه APT28، Fancy Bear یا Strontium مورد بهره‌برداری قرار گرفته، رسیدگی می‌کند.

آسیب‌پذیری با شناسه‌ی CVE-2016-7255 هفته‌ی گذشته توسط گوگل به‌طور عمومی افشاء شد. این افشای عمومی 10 روز پس از این صورت گرفت که گوگل این آسیب‌پذیری را به خود مایکروسافت اطلاع داده بود. این مسئله باعث ایجاد یک سری درگیری جزئی بین این دو شرکت شده بود.

گوگل در مورد آسیب‌پذیری‌هایی که به‌طور فعال مورد بهره‌برداری قرار می‌گیرند، به شرکت‌ها تنها 7 روز مهلت می‌دهد تا این آسیب‌پذیری را وصله کنند یا برای کاهش خطرات آن راه‌حل و مشاوره‌نامه منتشر کنند. ولی مایکروسافت با این قوانین گوگل مخالف است و معتقد است افشای یک آسیب‌پذیری با ذکر جزئیات، مشتریان را بیشتر در معرض خطر قرار می‌دهد.

بولتن امنیتی دیگری از ویندوز که باید در اولویت قرار گیرد بولتن MS16-132 است. این بولتن درجه‌ی اهمیت «جدی» دریافت کرده و چند آسیب‌پذیری اجرای کد از راه دور را برطرف می‌کند که شامل یک آسیب‌پذیری روز-صفرم نیز هست که در حال حاضر توسط مهاجمان مورد بهره‌بردرای قرار می‌گیرد.

این آسیب‌پذیری در کتابخانه‌ی فونت ویندوز قرار گرفته و با تعبیه‌ی فونت‌های جعلی در وب‌گاه‌ها و اسناد قابل بهره‌برداری است. مایکروسافت در این بولتن اشاره کرده است بهره‌برداری موفق از این آسیب‌پذیری به مهاجم امکان می‌دهد کنترل کامل سامانه‌ی آلوده را در دست گیرد.

3 آسیب‌پذیری دیگر که در اینترنت اکسپلورر و اج وجود داشتند در بولتن‌های MS16-142 و MS16-129 پوشش داده شده است. این آسیب‌پذیری‌ها قبل از اینکه وصله برای آن‌ها ارائه شود، به‌طور عمومی افشاء شده بود ولی به گفته‌ی خود مایکروسافت این آسیب‌پذیری‌ها در هیچ حمله‌ای مورد بهره‌برداری قرار نگرفته است.

بولتن مربوط به آفیس MS16-133 درجه‌ی مهم دریافت کرده اما چند آسیب‌پذیری اجرای کد از راه دور را پوشش

می‌دهد که این آسیب‌پذیری‌ها با اسناد جعلی خاصی قابل بهره‌برداری هستند.

آمل سارویت از شرکت امنیتی Qualys در تحلیل این وصله‌ها گفته است: «بخاطر اینکه استفاده از اسناد آفیس در شرکت‌ها بسیار متداول است، من فکر می‌کنم این بولتن باید درجه‌ی اهمیت «جدی» دریافت می‌کرد.»

مدیران SQL Server مایکروسافت نیز باید توجه ویژه‌ای به بولتن MS16-136 داشته باشند که آسیب‌پذیری‌هایی را در RDBMS engine، MDS API، سرویس تحلیل SQL و عامل SQL Server پوشش می‌دهد.

سارویت گفت: «آسیب‌پذیری‌های SQL Server تقریباً نادر هستند. هرچند که در آن‌ها آسیب‌پذیری اجرای کد از راه دور وجود ندارد، مهاجم می‌تواند امتیازات بالایی را بدست آورده و داده‌ها را ببیند، تغییر داده و حذف کند. همچنین می‌تواند حساب کاربری جدیدی ایجاد کند.»

اخبار فنی

قابلیت مدیریت از راه دور را در D-Link غیرفعال کنید

در سال 2016 هستیم و هنوز D-Link نتوانسته است پروتکل خودکار شبکه‌ی خانگی(HNAP) را بدرستی پیاده‌سازی کند. در مشاوره‌نامه‌ای کوتاه، بخش CERT کارنگی ملون می‌گوید سرویس HNAP در مسیریاب‌های سری DIR از شرکت D-Link دارای مشکل سرریز بافر مبتنی بر پشته هستند.

در این مشاوره‌نامه آمده است: «پردازش پیام ناقص SOAP زمانی که می‌خواهد عملیات ورود HNAP را اجرا کند منجر به سرریز بافر در پشته می‌شود. بخش‌های XML آسیب‌پذیر در بدنه‌ی پیام SOAP عبارتند از: Action، LoginPassword، Username و Captcha.»

باتوجه به اظهارات ارائه‌شده در این مشاوره‌نامه، D-Link هنوز به این مشکل رسیدگی نکرده است. این مسئله واحدهای DIR-823، DIR-822، DIR-818L(W)، DIR-880L، DIR-885L، DIR-890L، DIR-895L- و DIR-868L را تحت تأثیر قرار می‌دهد.

تنها راه‌حل موجود نیز غیرفعال کردن قابلیت مدیریت از راه دور است. متااسپلویت اثبات مفهومی این اشکال نیز از اینجا قابل مشاهده است.

ریبیرو محققی است که این اشکال را کشف کرده و گفته است بخش آسیب‌پذیر رشته‌ای با طول دلخواه را قبول کرده و در داخل پشته رونویسی می‌کند. پردازنده‌ی دستگاه آسیب‌پذیر از این پشته استفاده کرده و از عهده‌ی مدیریت آن برنمی‌آید و در نهایت دستگاه درهم شکسته می‌شود.

ریبیرو نوشته است برای درهم ریختن پشته دو روش وجود دارد: اولین راه این است که در بخش آسیب‌پذیر پیام، رشته‌ای با طول بزرگ‌تر از 3096 بایت ارسال شود. راه دوم نیز این است که پشته‌ی تابع فراخونی‌شده‌ی hnap_main با بیش از 2048 بایت اشغال شود.

این مسئله مشکل جدیدی نیست و از خیلی وقت پیش وجود داشته است. به‌طور مثال 6 سال پیش، گروه تحقیقات امنیتی SourceSec گزارش داد که اشکالی در پیاده‌سازی HNAP وجود دارد. همان‌طور که ریبیرو نیز اشاره کرد D-link سابقه‌ای طولانی در آسیب‌پذیری HNAP داشته است.

اخبار فنی

احراز هویت دومرحله‌ای بر روی دسترسی وب Outlook قابل دور زدن است

سازمان‌هایی که از Exchange Server استفاده کرده و فکر می‌کنند با پیاده‌سازی احراز هویت دومرحله‌ای که در دسترسی وب Outlook (OWA) وجود دارد، تحت یک لایه‌ی حفاظتی بیشتر قرار گرفته‌اند، باید بدانند که امنیت آن‌ها یک امنیت کاذب است.

یک ضعف در طراحی باعث شده تا یک مهاجم بتواند احراز هویت دومرحله‌ای را دور بزند و به فهرست مخاطبین، تقویم و رایانامه‌های یک شرکت دسترسی داشته باشد.

مسئله‌ی اصلی از جایی ناشی می‌شود که Exchange Server در کنار OWA واسط Exchange Web Services (EWS) را نیز ارائه می‌هد که در این واسط احراز هویت دومرحله‌ای پوشش داده نشده است. EWS به‌طور پیش‌فرض فعال است و از درگاه و کارگزار مشترک با OWA استفاده می‌کند به عبارت دیگر یک مهاجم با گواهی‌نامه‌های سرقتی می‌تواند از راه دور به EWS دسترسی یابد که بر روی زیرساخت یکسانی با OWA قرار دارد و مهاجم به صندوق ورودی رایانامه‌ی کاربران دسترسی خواهد داشت.

این موضوع روز چهارشنبه به‌طور عمومی توسط محقق کمال بولاک از شرکت امنیتی تپه‌های سیاه امنیت اطلاعات در داکوتای جنوبی فاش شد. بولاک یافته‌های خود را به‌طور خصوصی به مایکروسافت در 28 سپتامبر اعلام کرد و پس از تصدیق اولیه، پیگیری‌ها و رایانامه‌های پشت سر هم منجر به تولید یک وصله یا راه‌حلی برای کاهش خطرات این مسئله نشد.

بولاک چهارشنبه این مسئله را عمومی مطرح کرد و پس از مدت کوتاهی مایکروسافت با یک راه‌حلی برای کاهش خطر این موضوع با او تماس گرفت. بولاک به این وب‌گاه گفت که به احتمال زیاد مایکروسافت نمی‌تواند بدون معماریِ مجدد زیرساخت آسیب‌دیده، این مشکل را برطرف کند.

بولاک گفت: «مسئله‌ی بزرگی که وجود دارد این است که OWA بر روی کارگزار وب مشترک با EWS قرار دارد و هر دوی این سرویس‌ها به‌طور پیش‌فرض فعال هستند. مشکل بزرگی که فکر می‌کنم وجود دارد این است که بسیاری از افراد به نظر نمی‌رسد درکی از چیزی که دارد اتفاق می‌افتد داشته باشند. افراد فکر می‌کنند یک Exchange server بر روی اینترنت برای سرویس OWA دارند و نمی‌دانند که بر روی آن EWS نیز به‌طور پیش‌فرض فعال شده است. برای وصله‌ی این مشکل باید اطلاع‌رسانی بسیار گسترده‌ای صورت گیرد.»

بولاک معتقد است که اطلاع‌رسانی خوبی در خصوص این پیکربندی‌ها صورت نگرفته و افراد نمی‌دانند که پروتکل EWS نیز فعال بوده و از احراز هویت دومرحله‌ای پشتیبانی نمی‌کند.

بولاک گفت: «در مستندسازی‌های انجام‌شده واضح نیست که وقتی شما احراز هویت دومرحله‌ای را برای OWA

فعال می‌کنید هنوز پروتکل دیگری در کنار آن وجود دارد که احراز هویت یک مرحله‌ای دارد و هر دوی این پروتکل با زیرساخت داخلی یکسانی در ارتباط هستند.»

این محقق اشاره کرده است که این خیلی غیرمعمول نیست که دو پروتکل بر روی یک کارگزار در حال اجرا باشند و یکی از احراز هویت دومرحله‌ای پشتیبانی کند و دیگری نه. مثل پروتکل‌های RDP و SMB که بر روی یک کارگزار اجرا می‌شوند ولی هر دو بر روی یک درگاه یکسان کار نمی‌کنند و شرکت می‌تواند برای محدود کردن دسترسی، قوانین دیواره آتش را تنظیم کند.

بولاک توضیح داده است: «به همین دلیل این مسئله بسیار جدی است. وقتی شما یک کارگزار را در خارج از سازمان و در معرض عموم قرار می‌دهید و درگاهی را برای ارتباط با آن مشخص می‌کنید باید در نظر داشته باشید که پروتکل دیگری نیز بر روی این درگاه در حال اجراست و راه ارتباطی دیگری به زیرساخت‌های شما باز می‌شود.»

بولاک در گزارشی که منتشر کرد، توضیح داد چگونه حمله‌ای را علیه OWA حفاظت‌شده با احراز هویت دومرحله‌ای انجام داده است.

او با استفاده از یک حساب کاربری EWS و گواهی‌نامه‌های مربوط به آن و همچنین یک ابزار تست نفوذ با نام MailSniper توانسته است احراز هویت دومرحله‌ای OWA را دور بزند و بر روی صندوق ورودی رایانامه‌ی کاربران برای یافتن اطلاعات حساس به جستجو بپردازد. یک مهاجم در یک سناریوی واقعی از داده‌های افشاء شده‌ی برخط می‌تواند گواهی‌نامه‌های کاربران را بدست آورد.

برای اینکه تایید شود این مشکل مربوط به Duo for Outlook نیست، بولاک همین آزمون را بر روی Office 365 که بر روی آن قابلیت احراز هویت چندمرحله‌ای Azure مایکروسافت فعال بود، انجام داد و گفت که همچنان می‌تواند احراز هویت دومرحله‌ای را دور بزند.

سخنگوی مایکروسافت گفت: «این مشکل بر روی آفیس 365 که بر روی آن احراز هویت چندعاملی به‌طور کامل فعال شده باشد، تاثیر نمی‌گذارد. آنچه در وبلاگ توضیح داده شده آسیب‌پذیری نرم‌افزار نیست و بدون داشتن گواهی‌نامه و گذرواژه‌ی حساب کاربری کار نمی‌کند.»

بولاک گفت: «من فکر می‌کنم بهترین راه‌حل این است که این کارگزار مجدداً معماری شود. مایکروسافت باید سرویس EWS را به‌طور پیش‌فرض غیرفعال کند و اگر مشتری به آن نیاز داشت خودش آن را فعال کند. مایکروسافت می‌خواهد همه‌ی پروتکل‌ها را بر روی کارگزار خود داشته باشد و کار توسعه را راحت‌تر کند.»

فصل پنجم

اخبار تحـــلیلی

اخبار تحلیلی

آسیب‌پذیری‌های تراید‌نت iOS چه ویژگی‌هایی دارند؟

آسیب‌پذیری‌های روز صفرم «Trident» که صاحبان دستگاه‌های iOS را در معرض خطر قرار دادند در ماه آگوست وصله شدند، اما جزئیات کامل آن‌ها همین هفته منتشر شد.

این سه نقص مهم که محققان امنیتی آزمایشگاه سیتیزن و Lookout در ماه آگوست موفق به کشف آن‌ها شدند، توسط یک قطعه نرم‌افزار نظارتی مدرن به نام Pegasus مورد نفوذ واقع شده بودند؛ Pegasus به‌طور مخفیانه به دستگاه‌های iOS نفوذ می‌کند. این نرم‌افزار که در حقیقت توسط یک گروه فن‌آوری با مسئولیت محدود به نام NSO واقع در اسرائیل به فروش رسیده، به عنوان «پیچیده‌ترین حمله‌ی دیده‌شده روی نقاط پایانی» شهرت دارد.

این آسیب‌پذیری‌ها کاربران آیفون 4s و نسخه‌های بعد از آن، آی‌پد 2 و پس از آن، و نیز نسل پنجم از آی‌پاد تاچ و بعد از آن را در معرض خطر قرار می‌داد.

در روز ۲۵ ماه آگوست، اپل iOS 9.3.5 را منتشر کرد تا به این آسیب‌پذیری‌ها خاتمه دهد، اما فقط جزئیات اندکی از این شکاف‌ها را برملا کرد. در آن زمان جالب‌ترین نکته مربوط به نرم‌افزار Pegasus بود، نرم‌افزاری به سازمان‌های دولتی فروخته می‌شد و علیه روزنامه‌نگاران، فعالان سیاسی، مخالفان دولت، و اهداف دیگر در سراسر جهان به کار گرفته می‌شد.

در واقع اندکی پس از آن‌که اخبار مربوط به تراید‌نت به بیرون درز کرد، صنعت نظارتی مخفیانه‌ی رژیم صهیونیستی به کانون توجهات تبدیل شد. یک گزارش بین‌المللی و غیردولتی بریتانیایی در حوزه‌ی حریم خصوصی نشان داد که ۲۷ شرکت نظارتی در اسرائیل مستقر می‌باشند، همه‌ی این شرکت‌ها می‌بایست فن‌آوری‌های لازم برای مبارزه با جرایم و تروریسم را از طریق ابزارهای مجاز طراحی نمایند. با این وجود تردیدهایی درباره‌ی سوءاستفاده‌های احتمالی از این فن‌آوری وجود دارد.

این آسیب‌پذیری‌ها که شناسه‌های CVE-2016-4655، CVE-2016-4656 و CVE-2016-4657 به آن‌ها تعلق گرفته، اندکی بعد از انتشار وصله‌ی فوری iOS، در OS X و سافاری هم اصلاح شده‌اند.

حالا Lookout قصد دارد جزئیات کامل این سه آسیب‌پذیری را منتشر کرده و توضیح دهد که چگونه این زنجیره‌ی نفوذی (و آلودگی‌های ناشی از Pegasus) عمل می‌کند؛ این رویه با یک آسیب‌پذیری موجود در وب‌کیت سافاری شروع می‌شود، سپس با یک شکاف نگاشت هسته ادامه می‌یابد، در نهایت هم به یک خرابی حافظه‌ی هسته خاتمه می‌یابد که این نقص منجر به جیل‌بریک می‌شود. ساز و کار جاسوسی Pegasus نیز به این مراحل اضافه شده است.

آسیب‌پذیری نخست با آسیب رساندن به کتابخانه‌ی JavaScriptCore وب‌کیت ممکن است مورد سوءاستفاده

واقع شود، این سوءاستفاده زمانی رخ می‌دهد که کاربر روی یک پیوند اسپیرفیشینگ کلیک کند که مرورگر سافاری را باز می‌کند. با اجرای یک محتوای مخرب جاوااسکریپت در مرورگر، نفوذگر می‌تواند در فرآیند WebContent سافاری، کد دلخواه خود را به اجرا درآورد.

جاسوس‌افزار Pegasus به کمک دنباله‌ی مخصوصی از Propertyهای تابع defineProperties() می‌تواند از این آسیب‌پذیری سوءاستفاده کند. این نرم‌افزار تلاش‌های متعددی را برای بهره‌برداری از این شکاف صورت می‌دهد، سپس ابزارهایی را برای اجرای محلی کد دلخواه خود و نیز ساخت یک نگاشت اجرایی حاوی محتوای کد مخرب راه‌اندازی می‌کند.

پس از آن‌که مرحله‌ی نخست حمله کامل شد، مرحله‌ی دوم راه‌اندازی می‌شود تا از یک شکاف افشای اطلاعات هسته با شناسه‌ی CVE20164655 بهره‌برداری به عمل آید. این موضوع وقتی رخ می‌دهد که نرم‌افزار مخرب این ماجرا سعی کند در آیفون قربانی یک تشدید امتیاز را صورت دهد و مقدمات لازم را برای مرحله‌ی نهایی که منجر به جیل‌بریک آیفون می‌شود، مهیا سازد.

محققان امنیتی متوجه شدند که نرم‌افزار Pegasus سعی می‌کند روی دستگاه‌های تحت نفوذ حضور مستمری داشته باشد و به این منظور روی دو موضوع مجزا تکیه دارد: وجود این سرویس rtbuddyd و یک آسیب‌پذیری در کد JavaScriptCore. موضوع نخست به جاسوس‌افزار اجازه می‌دهد تا کد را در مرحله‌ی بوت یا راه‌اندازی اجرا کند، و از مورد دوم برای اجرای کد jsc و اجرای کد بدون امضاء برای سوءاستفاده‌ی مجدد از هسته بهره‌برداری نماید.

اخبار تحلیلی

تروجان بانکی TrickBot مجهزتر می‌شود

تروجان بانکی TrickBot، که بیشترین شباهت را با Dyre دارد، یک فهرست بلندبالا از اهداف و نیز روش‌های دست‌کاری مرورگر را دارا می‌باشد.

محققان انتظار دارند که میزان آلودگی ناشی از این بدافزار و نیز حملات وابسته به آن تشدید شده باشد و کسب و کار و حساب‌های کاربری شرکت‌ها به هدف نخست آن مبدل شده باشند.

TrickBot به سرعت و ظرف مدت سه ماه و در طول مرحله‌ی آزمون و توسعه‌ی خود به رشد و نمو رسید. این تروجان بانکی همچنین دو روش فوق پیشرفته‌ی ویرایش مرورگر را که در سال‌های گذشته در سایر بدافزارهای بانکی نیز رؤیت شده، در خود تعبیه کرده است.

TrickBot دارای ارتباط نزدیکی با بدافزار بانکی Dyre است؛ بسیاری از ویژگی‌ها و کدهای زیرساختی این دو تروجان با یکدیگر مشترک است. به نظر می‌رسد TrickBot با حملات ابتدایی علیه بانک‌های استرالیا بی‌ارتباط نباشد، در این حملات نیز مانند کد بدافزار Dyre چند مورد تزریق کد مشاهده شده است؛ البته عوامل پشت پرده‌ی بدافزار Dyre در حال حاضر در زندان روسیه به سر می‌برند.

کارشناسان می‌گویند TrickBot قابلیت‌های تازه‌ای را به کار گرفته و اهداف تازه‌ای را پیدا کرده است، از جمله‌ی این اهداف می‌توان به وب‌گاه‌های بانکی تجاری مؤسسات مالی در انگلستان، استرالیا، نیوزلند، کانادا، و آلمان اشاره کرد. نفوذگران دست‌اندرکار TrickBot در وهله‌ی اول روی حملات تغییر مسیر و نیز تزریق کد سمت کارگزار به تعداد انگشت‌شماری از بانک‌ها تمرکز کرده‌اند، اما گزارش ماه نوامبر IBM باعث شد تا فوت و فن این بدافزار عوض شود.

دامنه‌ی عمل‌کرد TrickBot یک‌شبه دگرگون شد، متصدیان این تروجان دو پیکربندی تازه را در اوایل ماه نوامبر برای TrickBot پیاده‌سازی کردند؛ این تحول چیزی بیش از اضافه کردن URL به پیکربندی این بدافزار بود؛ روشی که علیه بانک‌های انگلستان به کار گرفته شد تا حملات تغییر مسیر سفارشی در آن‌ها صورت بگیرد، این شیوه در حقیقت پیشرفته‌ترین روش برای دست‌کاری چیزی است که کاربر در مرورگر مشاهده می‌کند.

محققان می‌گویند براساس بررسی‌های صورت‌گرفته روی TrickBot و سرعت توسعه‌ی آن می‌توان گفت، مجرمان متصدی آن با دقت هرچه تمام‌تر تغییر مسیرها را به منظور ارائه در کمپین‌های این تروجان، و نیز خرید آسان آن‌ها از باندهای مخرب دیگر از پیش در نظر گرفته‌اند.

این تروجان برخلاف Dyre از نظر راه‌اندازی تبلیغات مخرب به کمک بسته‌ی نفوذی RIG، ضمیمه‌های مخرب رایانامه‌ها، و نیز ماکروهای آلوده‌ی آفیس که از طریق «بارکننده‌ی Godzilla» ارائه می‌شود، تقویت شده است. این ویژگی‌ها نشان می‌دهد که گروه پشتیبان TrickBot

به دنبال حساب‌های تجاری خاصی است. این گروه هرزنامه‌های مملو از بدافزار را به کمپین‌ها می‌فرستد و به موج رایانامه‌های بی‌دردسر اکتفا نمی‌کند. ظاهراً TrickBot از تحول دست برنمی‌دارد. روش‌های آلوده‌سازی این تروجان در هر زمانی متفاوت است. به نظر می‌رسد که تکامل پیوسته‌ی TrickBot به این واقعیت ربط داشته باشد که عوامل مخرب پشت پرده‌ی آن در شبکه‌ی توزیع‌کننده‌ی بدافزار و باتنت دیگری نیز فعالیت دارند. نمونه‌ای از TrickBot که مورد تحلیل واقع شده دربرگیرنده‌ی یک بارکننده‌ی سفارشی به نام TrickLoader است، از این بارکننده در ربات هرزنامه‌ی Cutwail هم استفاده شده بود، به گفته‌ی پژوهش‌گران این بارکننده نیز مشابه همان موردی است که باند Dyre در کمپین هرزنامه‌ی خود استفاده می‌کردند.

اخبار تحلیلی

کالبدشکافی کیت بهره‌برداری RIG

کیت بهره‌برداری سودآور این روزها RIG جای خالی کیت‌هایی همچون Angler، Neutrino و Nuclear را پر کرده است. وقتی حرف از کیت‌های بهره‌برداری به میان می‌آید RIG در مقام اول قرار دارد. اکنون محققان سیسکو تالوس در تلاش هستند بررسی بیشتری بر روی این کیت قوی انجام داده و توسعه‌هایی که بر روی این کیت داده می‌شود را بتوانند خنثی کنند.

به عنوان یک اصل برای کاهش نرخ آلودگی به کیت‌ها، اول باید مسیر آلوده شدن قربانی را تشخیص داد و فهمید که چگونه سازوکارهای امنیتی در نرم‌افزار و تجهیزات دور زده شده است.

در بررسی دقیقی که اخیراً توسط محققان سیسکو تالوس بر روی RIG انجام شده، ویژگی‌های منحصربفردی از این کیت کشف شده است. به‌طور خلاصه مثل هر کیت دیگری، عوامل RIG نیز از دروازه‌هایی استفاده می‌کنند تا قربانیان را به سمت کیت بهره‌برداری خود هدایت کنند. چیزی که RIG را منحصربفرد می‌کند ترکیب فناوری‌های مختلف وب مانند DoSWF، جاوا اسکریپت، فلش و اسکریپت ویژوال بیسیک برای مبهم‌سازی حمله است.

مسئله‌ی بدتری که وجود دارد این است که در هر سناریوی حمله، به‌طور پویا رمزنگاری و کدگذاری پرونده‌های انتقالی تغییر پیدا می‌کند. این روش تضمین می‌کند هر سری که جلسه‌ی حمله‌ی جدیدی آغاز می‌شود، اسکریپت شکلی متفاوت خواهد داشت و مهاجمان مطمئن هستند که با الگوریتم‌های ساده‌ی انطباق رشته و یا مقدار درهم‌سازی، تشخیص داده نخواهند شد.

محققان می‌گویند در دل هر حمله‌ی RIG سه حمله‌ی مجزا وجود دارد که از حملات جاوا اسکریپت، فلش و اسکریپت ویژوال بیسیک استفاده می‌کند.

وقتی زمان تحویل پرونده‌ی بدافزار فرا می‌رسد، کیت RIG بدافزار مورد نظر را چندین بار بر روی رایانه‌ی قربانی نوشته و اجرا می‌کند. اگر یکی از این روش‌ها کار نکند و یا توسط سازوکارهای امنیتی مسدود شود، روش‌های پشتیبان دیگری وجود دارد. تمامی این مراحل و روش‌ها نیز کم و بیش مبهم‌سازی شده‌اند.

گفته می‌شود بیشترین آلودگی به این کیت از سمت وب‌گاه‌های آلوده است. وب‌گاه‌های زیادی وجود دارد که مورد نفوذ واقع شده‌اند و مهاجمان کد مخربی را در این وب‌گاه قرار داده‌اند که کاربران را به سمت دروازه‌ی دریافت کیت هدایت می‌کند. این دروازه‌ها نیز کاربران را به سمت صفحه‌ی اصلی کیت هدایت خواهند کرد.

چند پویش هم مشاهده شده که از دروازه‌هایی با روش‌های تبلیغ‌افزاری استفاده کرده‌اند و قربانی به سمت ترافیک مخرب مهاجمان هدایت شده است. در این حالت قربانی با حجم انبوهی از حملات جاوا اسکریپت، فلش و اسکریپت ویژوال بیسیک مواجه خواهد شد. در انتها نیز

تمامی این اسکریپت‌ها پرونده‌ی بدافزار را بر روی ماشین قربانی بارگیری و اجرا می‌کنند. این بدافزار همانی است که کیت بهره‌برداری قصد تحویل آن را داشته است.

اولین مرحله از حمله کشاندن ترافیک به سمت یک وب‌گاه آلوده است که فرآیند هدایت را آغاز می‌کند. وب‌گاه آلوده یک پرونده‌ی فلش (SWF) را بارگذاری می‌کند. در ادامه این پرونده‌ی فلش یک یا دو iFrames را بر روی وب‌گاه آلوده درج می‌کند. الان است که قربانی از طریق این iFrames به سمت دروازه‌ی کیت بهره‌برداری هدایت می‌شود.

این دروازه که چیزی بیش از یک وب‌گاه یا کارگزار نیست، مجدداً قربانی را به سمت صفحه‌ی دیگری که کیت بهره‌برداری بر روی آن میزبانی می‌شود، هدایت می‌کند. صفحه‌ی آخری که کیت بهره‌برداری را میزبانی می‌کند حاوی 3 جاوا اسکریپت متفاوت است. یک جاوا اسکریپت بهره‌برداری فلش را بارگیری می‌کند، دیگری اسکریپت ویژوال بیسیک را و آخری نیز خود حاوی یک بهره‌برداری است. همان‌طور که مشاهده می‌شود چرخه‌ی آلودگی بسیار پیچیده بوده و در تمامی مراحل مبهم‌سازی صورت گرفته است.

پرونده فلش به شدت با استفاده از یک نرم‌افزار محافظت تجاری با نام DoSWF که پرونده‌های فلش را رمزنگاری می‌کند، مبهم شده است. این پرونده‌ی فلش دو iFrames بر روی وب‌گاه آلوده ایجاد می‌کند. اولین iFrames فوراً ایجاد شده و دیگری پس از گذشت زمان مشخصی ساخته می‌شود.

هنوز دلیل این تاخیر در ایجاد iFrames مشخص نشده است ولی تصور می‌شود نوعی سازوکار پشتیبانی برای حالتی باشد که نمونه اول موفق نشده است.

در ادامه با توجه به آسیب‌پذیری که در مرورگر قربانی وجود دارد، کد جاوا اسکریپتی که در داخل iFrame ها قرار دارد، قربانی را به سمت صفحه‌ی کیت RIG هدایت می‌کند. اینجاست که مرورگر قربانی با 3 اسکریپت مخفی که در داخل متغیرهای جاوا اسکریپت تعبیه شده، مواجه می‌شود.

یکی از این اسکریپت‌ها اسکریپت ویژوال بیسیک است که پس از آزمون‌های مختلف بر روی سامانه‌ی هدف، تابع DoMagic() را اجرا می‌کند و بار داده‌ی بدافزار بارگیری می‌شود.

اسکریپت دوم دارای قابلیتی است که دستورات تصادفی را بین کدهای جاوا اسکریپت قرار می‌دهد. این دستورات در هر جلسه تغییر می‌کند و دلیل این کار متفاوت بودن کدگذاری Base64 در هر جلسه است. این اسکریپت در ادامه مجدداً یک پرونده‌ی فلش را که با DoSWF رمزنگاری شده، اجرا می‌کند. محققان سیسکو تالوس تلاش دارند تا این اسکریپت را از حالت مبهم خارج کنند و نتیجه‌گیری آن‌ها تا به الان این است که این اسکریپت حاوی کد شِل است که در زمان اجرا کدگشایی شده و با رشته‌ای دیگر از پرونده‌ی SWF ترکیب می‌شود و در نهایت بهره‌برداری را اجرا می‌کند.

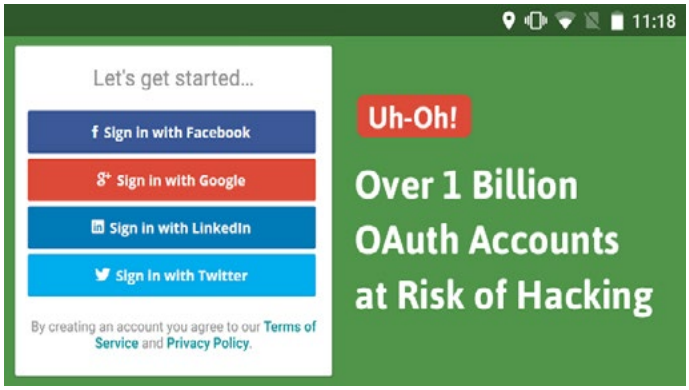
آخرین اسکریپت موجود در این کیت از آسیب‌پذیری با شناسه‌ی CVE-2013-2551 با نام مستعار MS13-037 برای آلوده کردن قربانی استفاده می‌کند. براساس بولتن امنیتی مایکروسافت در ماه می 2013 این آسیب‌پذیری مربوط به اینترنت اکسپلورر و سریز عدد صحیح است. این آسیب‌پذیری شامل کدی است که قربانی را به سمت بارگیری بدافزار نهایی هدایت می‌کند.

در پویش‌هایی که سیسکو تالوس برای تهیه‌ی این گزارش بررسی کرده است، بار داده‌ی بدافزار شامل باج‌افزار (باج‌افزارهایی همچون CRYPTFILE2، Locky و CryptXXX)، تروجان (Gamarue و Gootkit) و چند پرونده‌ی اجرایی ناقص بوده است.

سیسکو تالوس برای حفاظت در برابر RIG توصیه کرده تا تمامی افزونه‌های غیرضروری بر روی مرورگرها را غیرفعال کنید. وصله و به‌روزرسانی مرورگرها و افزونه‌ها نیز بسیار ضروری است. هر مرورگری با افزونه‌ی فلشِ وصله‌نشده به احتمال زیاد آلوده خواهد شد.

اخبار تحلیلی

ورود به 1 میلیارد حساب کاربری بر روی برنامه‌های تلفن همراه با استفاده از پروتکل OAuth



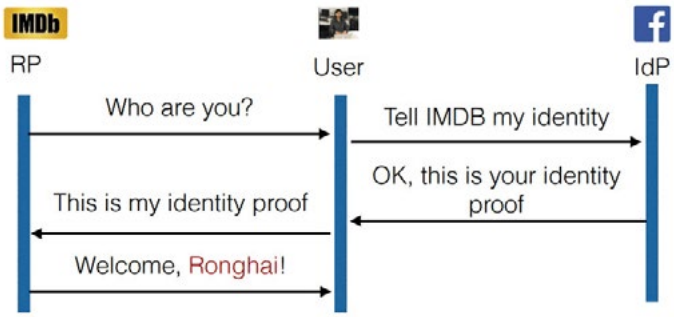
محققان امنیتی روشی را کشف کردند که بسیاری از برنامه‌های اندروید و iOS را هدف قرار داده و به مهاجمان اجازه می‌دهد بدون اطلاع قربانی به حساب‌های کاربری که بر روی تلفن همراه او وجود دارد، وارد شوند.

سه محقق از دانشگاه چینی هنگ‌کنگ دریافتند که بسیاری از برنامه‌های مشهور تلفن همراه که دارای ورود یک مرحله‌ای هستند، OAuth 2.0 را به‌شکل ناامنی پیاده سازی کرده‌اند.

OAuth 2.0 یک استاندارد باز برای احراز هویت است که به کاربران اجازه می‌دهد با استفاده از حساب کاربری گوگل، فیس‌بوک و یا حساب کاربری Sina (یک شرکت چینی) به سایر سرویس‌های شخص ثالث وارد شوند. این ویژگی کاربر را قادر می‌سازد بتواند بدون داشتن نام کاربری و گذرواژه‌ی اضافی به هر سرویسی وارد شود.

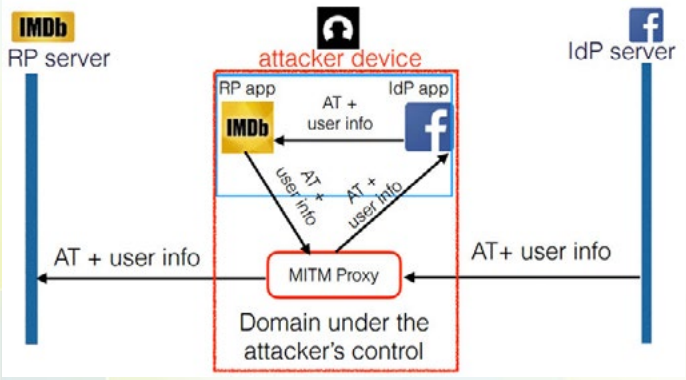
توسعه‌دهندگان چگونه باید OAuth را پیاده‌سازی کنند؟ (روش صحیح)

زمانی که کاربر می‌خواهد به برنامه‌ی ثالثی از طریق OAuth وارد شود، برنامه یک شناسه‌ی ارائه‌دهنده مثلاً فیسبوک را درخواست می‌کند. اطلاعات حساب کاربری مربوط به فیس‌بوک بررسی می‌شود و اگر درست بود یک توکن دسترسی از فیس‌بوک برای OAuth صادر می‌شود که این توکن در ادامه به کارگزار برنامه‌ی ثالث تحویل داده می‌شود.



زمانی‌که توکن صادر شد، کارگزار برنامه‌ی مورد نظر اطلاعات مربوط به احراز هویت فیس‌بوک را درخواست می‌کند و اگر این اطلاعات درست بود پس از تایید، کاربر از طریق این گواهی‌نامه‌ها می‌تواند به این سرویس جدید وارد شود.

طوری که توسعه‌دهندگان OAuth را پیاده‌سازی می‌کنند؟ (روش اشتباه)



محققان دریافتند که بسیاری از توسعه‌دهندگان برنامه‌های تلفن همراه، اعتبار اطلاعات ارسالی از سمت ارائه‌دهنده‌ی شناسه مانند فیس‌بوک، گوگل و سینا را بررسی نمی‌کنند.

کارگـزار برنامـه به‌جـای اینکـه اطلاعـات OAuth (توکـن دسترسـی) کـه بـه همـراه اطلاعـات احـراز هویـت کاربـر ضمیمـه شـده را بررسـی کنـد و ببینـد کـه آیـا ایـن دو بـا هـم ارتباطـی دارنـد، تنهـا شناسـه‌ی کاربـر کـه در شناسـه‌ی ارائه‌دهنـده وجـود دارد را بررسـی می‌کنـد.

بـا توجـه بـه ایـن اشـتباهی کـه رخ داده، یـک مهاجـم بـه راحتـی می‌توانـد برنامـه‌ی آسـیب‌پذیر را بارگیـری کـرده و بـا اطلاعـات خـود بـه ایـن برنامـه وارد شـود. در ادامـه نیـز نـام کاربـری خـود را بـه نـام کاربـری قربانـی تغییـر دهـد و کارگـزاری را تنظیـم کنـد تـا اطلاعـات ارسال‌شـده از سـمت گـوگل، فیس‌بـوک یـا سـینا و یـا هـر ارائه‌دهنـده‌ی دیگـری را ویرایـش کنـد. وقتـی ایـن کارهـا انجـام شـد، کنـترل تمامـی داده‌هـای موجـود در ایـن برنامـه، در اختیـار مهاجـم خواهـد بـود.

ایـن حملـه چـه اثراتـی می‌توانـد داشـته باشـد؟ اگـر مهاجـم بـه برنامـه‌ی سـفر قربانـی وارد شـده باشـد، می‌توانـد برنامه‌ریـزی قربانـی را بفهمـد. اگـر وارد برنامـه‌ی هتـل شـده باشـد، می‌توانـد اتاقـی را رزرو کنـد و هزینـه‌ی آن را بـا حسـاب قربانـی پرداخـت کنـد. همچنیـن مهاجـم بـه راحتـی می‌توانـد اطلاعاتـی همچـون آدرس و جزئیـات کارت بانکـی کاربـر را بـه سرقـت بـبرد.

پروتـکل OAuth بسـیار پیچیـده اسـت و توسـعه‌دهندگان برنامه‌هـای تلفـن همـراه نیـز خیلـی توانمنـد نیسـتند و اگـر از ایـن پروتـکل بـه درسـتی اسـتفاده نکننـد، برنامه‌هـای آن‌هـا کامـلاً بـاز خواهـد بـود.

محققـان صدهـا برنامـه‌ی محبـوب تلفـن همـراه را پیـدا کردنـد کـه از سرویـس ورود تک‌مرحلـه‌ای (SSO) پشـتیبانی می‌کننـد و 2.4 میلیـارد بـار بارگیـری شـده‌اند و دارای چنیـن آسـیب‌پذیری هسـتند.

محققـان بهره‌بـرداری از ایـن آسـیب‌پذیری را بـر روی آیفـون بررسـی نکرده‌انـد امـا معتقدنـد کـه ایـن حملـه بـر روی هـر برنامـه‌ی آسـیب‌پذیر بـر روی سـامانه‌ی عامـل iOS اپـل نیـز کار خواهـد کـرد.

ایـن محققـان مقالـه خـود را بـا عنـوان «ورود بـه 1 میلیـارد حسـاب کاربـری بـر روی برنامه‌هـای تلفـن همـراه بـا اسـتفاده از OAuth2.0» روز جمعـه در کنفرانـس بلک‌هـت اروپـا ارائـه کردنـد.

اخبار تحلیلی

سرقت اطلاعات حساس از ماشین مجازی با حملات آدرس‌دهی DRAM

آندرس فوگ، تحلیلگر بدافزار و مایکل شوارتز، دانشجوی دکتری در دانشگاه صنعتی گراتس در اتریش مشکلات امنیتی در طراحی فعلی DRAM را تشریح کرده و برخی حملات عملی cross-CPU را نشان دادند. بخش اول از این تحقیق در ماه آگوست در 25امین سمپوزیوم امنیت USENIX ارائه شده بود.

در کنفرانس 2016 بلک‌هت اروپا، این محققان نشان دادند چگونه می‌توان اطلاعات حساس و خیلی کوچک همچون گذرواژه و یا کلید خصوصی را از روی ماشین مجازی بدون داشتن دسترسی به شبکه و تنها از طریق کد جاوا اسکریپتی که بر روی مرورگر میزبان اجرا می‌شود، به سرقت برد. آن‌ها همچنین بهبودی برای حملات Rowhammer ارائه کرده و نشان دادند برخلاف چیزی که قبلاً تصور می‌شد، این روش علیه DDR4 نیز کار می‌کند. استفاده از آدرس مجازی این امکان را می‌دهد تا بر روی یک CPU چند پردازه به‌طور امن اجرا شوند. با این وجود وقتی در مورد DRAM صحبت می‌شود، CPU به آدرس فیزیکی نیاز دارد و باید آدرس‌های مجازی به آدرس فیزیکی نگاشت شوند.

تابع نگاشتی که توسط کنترلر حافظه‌ی پردازه‌ها استفاده می‌شود، مستندسازی نشده است اما گروه فوگ و شوارتز با موفقیت توانستند این مسئله را با اندازه‌گیری زمانی که طول می‌کشد CPU داده‌ها را از بانک حافظه بخواند، مهندسی معکوس نمایند. یک ابزار نیز برای مهندسی معکوس این تابع نگاشت توسط محققان این گروه به‌صورت متن‌باز منتشر شده است.

برخلاف حملات حافظه‌ی نهان که مدت زیادی است کشف شده و کارشناسان راه‌های مقابله با آن را ارائه کرده‌اند، حملات DRAMA مزایای کار با CPU را دارند. با این وجود شباهت‌هایی هم بین این حملات وجود دارد. محققان در مقاله‌ی خود توضیح دادند: «ما فهمیدیم بافرهایی که در DRAM استفاده شده، رفتار مشابهی با حافظه‌ی نهان CPU دارند. ما با بهره‌برداری از اختلاف زمانی در بافرهای DRAM حمله را اجرا می‌کنیم. استفاده از اختلاف زمان تحت عنوان حملات حافظه‌ی نهان شناخته می‌شود. بزرگ‌ترین مزیت حمله‌ی DRAM این است ک به هیچ حافظه‌ی اشتراکی نیاز ندارد. علاوه بر این در بیشتر تنظیمات، حافظه‌ی اصلی بین CPU ها به اشتراک گذاشته شده است و ما می‌توانیم چنین حمله‌ای را در سناریوهای cross-CPU انجام دهیم.»

این دو محقق نشان دادند بدون اجرای بایتری بر روی سامانه‌ی میزبان و بدون بهره‌برداری از هیچ آسیب‌پذیری، می‌توانند یک کانال مخفی بین ماشین مجازی و میزبان باز کنند. فرستنده که در داخل ماشین مجازی اجرا می‌شود و گیرنده که بر روی مرورگر میزبان در حال اجرا شدن است، بر روی یک بانک حافظه توافق می‌کنند که

این حافظه می‌تواند هارکد شود. زمان‌های دسترسی به حافظه اندازه‌گیری می‌شود و اگر سرعت دسترسی سریع باشد یک بیت «0» و اگر دسترسی کُند باشد یک بیت «1» ارسال می‌شود.

محققان همچنین نشان دادند چگونه با استفاده از این روش می‌توانند کلیدهایی که بر روی ماشین مجازی فشرده می‌شود را به سرقت ببرند. در این سناریو مهاجم باید سامانه را کاملاً شناسایی کند تا بداند دقیقاً چه اتفاقاتی را می‌خواهد جاسوسی کند. مهاجمان می‌توانند قربانی را تحریک کنند تا یک صفحه‌ی وب حاوی جاوا اسکریپت مخرب را ببیند یا از حملات تبلیغ‌افزاری استفاده کنند.

محققان اشاره کردند که این احتمال وجود دارد که حافظه‌ای که قرار است داده‌ها از آن خارج شوند، توسط برنامه‌ی دیگری استفاده شود که در این صورت داده‌ها خراب خواهند شد. ولی این احتمال خیلی کم است و برای جلوگیری از این اتفاق یک کد تشخیص خطا پیاده‌سازی شده است. برای اینکه خارج کردن داده‌ها به شکل مؤثرتری انجام شود، داده‌ها در قالب بسته‌هایی ارسال می‌شوند. این بسته‌ها حاوی دنباله‌ی بیتی هستند که مشخص می‌کند آیا این بسته جدید است یا بسته‌ای است که ارسال مجدد می‌شود.

در حمله‌ی جاوا اسکریپت محققان به نرخ انتقال 11 کیلوبیت بر ثانیه دست یافته‌اند. با این حال این حمله اگر با کد محلی پیاده‌سازی شود و بخشی از بدافزار بر روی دامنه‌ی محافظت‌شده (همچون ماشین مجازی) و بخشی از بدافزار بر روی میزبان در حال اجرا باشد، نرخ انتقال به 600 کیلوبیت بر ثانیه و حتی بیشتر نیز می‌رسد اگر که CPU یکسانی استفاده شود.

هرچند که تمرکز اصلی محققان بر روی معماری اینتل x86-64 بوده است ولی آن‌ها تایید کرده‌اند که این مشکل بر روی سایر معماری‌ها نیز وجود دارد و این مشکل اصلی مربوط به RAM است. این مشکل همچنین پردازنده‌های ARM که بر روی تلفن‌های هوشمند استفاده می‌شود را تحت تأثیر قرار می‌دهد.

بخاطر اینکه این مشکلات از طراحی و عملکرد DRAM ناشی می‌شود، محققان فکر می‌کنند که به راحتی نمی‌توان این مشکل را برطرف کرد و کاهش داد. آن‌ها همچنین اشاره کردند درست است که این آسیب‌پذیری بسیار جدی است ولی بعید است که در چند روز آینده شاهد این باشیم که از این آسیب‌پذیری بهره‌برداری شود. هدف از این پژوهش افزایش آگاهی بوده است تا نشان داده شود که سخت‌افزار نیز نیاز به امنیت دارد و تمامی مشکلات مربوط به نرم‌افزار نیست.

اخبار تحلیلی

آغاز تماس تلفنی با بهره‌برداری از آسیب‌پذیری WebView

توسعه‌دهندگان برنامه‌های iOS که از WebView استفاده کرده‌اند باید در جریان یک اشکال قابل بهره‌برداری باشند که اجازه‌ی تماس تلفنی به شماره‌ای که مهاجم انتخاب می‌کند را می‌دهد.

محقق امنیتی با نام کالین مولینر گفته است که بهره‌برداری از این آسیب‌پذیری بسیار ساده است و تنها به یک خط کد HTML نیاز دارد. خطراتی که کاربر را تهدید می‌کند بالا بردن شارژ برای شماره‌های پولی و یا بدتر از این اجرای حملات منع سرویس است. شبیه به اتفاقی که هفته‌ی قبل برای یک مرد آریزونایی افتاد و او بخاطر به اشتراک گذاشتن یک بهره‌برداری بر روی یوتیوب به زندان افتاد. این بهره‌برداری به کاربران اجازه می‌داد تنها با یک کلیک تماس‌های سیل‌آسایی با مرکز تلفن 911 برقرار کنند.

مولینر گفت برنامه‌های معروف iOS همچون توییتر و لینکدین در برابر این حمله آسیب‌پذیر هستند. این محقق گفته است برنامه هایی همچون فیس بوک، واتس‌اپ، اسنپ‌چت و پِلپ را نیز بررسی کرده و هیچ یک از این برنامه‌ها در معرض خطر نبوده‌اند. مولینر هشدار داده که تنها برنامه‌های معروف iOS را بررسی کرده و به احتمال زیاد، تعداد بیشتری از برنامه‌ها در برابر این اشکال آسیب‌پذیر هستند.

مولینر گفت: «تعداد زیاد پیام‌رسان و رسانه‌ی اجتماعی دیگر وجود دارد که پتانسیل آسیب‌پذیری در برابر این اشکال را دارند. هر برنامه‌ای که در کد خود WebView را داشته باشد که از طریق آن URL بارگیری شود، پتانسیل آسیب‌پذیری دارد. بهره‌برداری از آن نیز بسیار ساده است و هرکسی می‌تواند آن را انجام دهد.»

مولینر به‌محض اینکه از وجود این اشکال آگاه شد آن را به‌طور خصوصی به توییتر اطلاع داد و در پاسخ به او گفته شد که این مشکل یک آسیب‌پذیری تکراری است. پس از این ماجرا این محقق آسیب‌پذیری را به‌طور عمومی افشاء کرد. او همچنین تلاش کرد این مسئله را به برنامه‌ی پاداش در ازای اشکال لینکدین نیز گزارش کند ولی بعداً فهمید که این یک برنامه‌ی خصوصی است و یکی از اعضای گروه امنیتی لینکدین بر روی این مسئله کار می‌کند. اپل نیز گزارش ارائه‌شده توسط مولینر را تایید کرد و گفت به این مشکل رسیدگی خواهد کرد.

برای بهره‌برداری از این آسیب‌پذیری، مهاجم صرفاً نیاز دارد تا پیوندی را برای قربانی ارسال کند. این پیوند قرار است قربانی را به صفحه‌ی وبی که کد HTML مهاجم میزبانی می‌شود، هدایت کند. این کد از طریق شماره‌گیری بر روی دستگاه، تماسی را آغاز خواهد کرد که این عمل مشابه نمونه‌ای است که مولینر در سال 2008 به توییتر گزارش داد. این محقق گفت می‌تواند با نمایش یک برنامه‌ی ثانویه بر روی صفحه‌ی نمایش که روی صفحه‌ی شماره‌گیری را می‌پوشاند، مانع از این شود که قربانی

تماس را قطع کند. در گزارشی که روز چهارشنبه منتشر شد مولینر عنوان کرد که کد قدیمی او همچنان کار می‌کند. او گفت که تنها یک خط کد HTML شماره‌گیری را آغاز کرده و 10 خط کد دیگر این حمله را مخفی می‌کند.

مولینر گفت: «من فکر می‌کردم این مشکل 8 سال پیش حل شده است. ولی ظاهراً هنوز پابرجاست. شما برای بهره‌برداری از این آسیب‌پذیری به نرم‌افزار خاصی نیاز ندارید. تنها یک نسخه آیفون که بر روی آن توییتر یا لینکدین نصب شده است و توانایی میزبانی کد HTML برای بهره‌برداری کافی است.»

مولینر در گزارش خود آنچه که در پشت پرده‌ی این حمله می‌گذرد را اینگونه توضیح داد:

«حدس من این است که زیرسامانه‌ی IPC در جابجایی چند کیلوبایت داده‌ی URL از طریق لایه‌های مختلف برنامه با مشکلاتی مواجه است و برنامه‌ی مورد هدف از مدیریت URL های طولانی خیلی راضی نیست. من در ادامه کدها را آورده‌ام. در این کد از ترکیب تگ meta-refresh- و window.location برای اجرای حمله استفاده می‌شود. این کد در ایجاد window.location سیزده ثانیه تأخیر ایجاد می‌کند تا مطمئن شود اول شماره‌گیری صورت گرفته است. این تأخیر نمی‌تواند خیلی طولانی باشد در غیر این‌صورت WebView مدیریت URL برای اجرای برنامه‌ی پیام را اجرا نخواهد کرد. در واقع شما باید زمان درست را رعایت کنید.»

در ادامه مولینر نمونه ویدئوهای حمله به توییتر و لینکدین را به اشتراک گذاشته است.

Expert Bulletin News

Information Communication Technology

2th year 2016 | Weekly bulletin

اخبار فناوری اطلاعات و ارتباطات

هفته نامه | شماره هشتاد و ششم | سال دوم | ۸۸ صفحه

خبرنامه هفتگی کارشناسی

مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج