شماره پنجم - خرداد ۱۳۹۶

خبرنامه "آپا" دانشگاه خوارزمی

در این شماره خواهید خواند:

صدور ۳۰۰۰۰ گواهی اعتبار سنجی به اشتباه!

بعد از اینکه معلوم شد شرکت Symantec در چند سال گذشته ۳۰۰۰۰ گواهیِ تمدید اعتبارسنجی (EV) نادرست صادر کرده است، شرکت گوگل برنامه ی خود برای مجازات این شرکت بابت ایجاد بی‌اعتمادیِ تدریجی به گواهی‌های SSL آن را اعلام کرد.

وضعیت کلیه‌ی گواهی‌های EV منتشرشده توسط مقامات Symantec حداقل برای یک سال به رسمیت شناخته نخواهد شد تا اینکه Symantec فرایند صدور گواهی‌های خود را اصلاح کند تا دوباره قابل اعتماد شود.

انتظار می‌رود که گواهی های تمدید اعتبارسنجی بیشترین سطح از اعتماد و احراز هویت (authentication) را داشته باشند زیرا قبل از صدور گواهی، مرجع صادرکننده‌ی گواهی باید هویت (identity) و وجود قانونیِ (legal existence) نهاد درخواست‌کننده را بررسی کند.

این حرکت بلافاصله بعد از اینکه Ryan Sleevi، مهندس نرم‌افزار تیم گوگل کروم، اطلاعیه‌ی زیر را در یک forum آنلاین منتشر کرد، انجام شد. اطلاعیه از این قرار بود:

"این بار نیز ، شاهد یک سری از نقص هایی همراه بود که ذیل مجموعه‌ی گواهی های اشتباه صادر شده ی قبلی از طرف Symantec هستیم، که باعث شده است دیگر هیچ اعتمادی به سیاست‌های صدور این گواهی و اقدامات Symantec در طی چند سال گذشته نداشته باشیم."

یکی از مهم‌ترین بخش‌های اکوسیستمِ SSL، اعتماد است. اما اگر CA ها قبل از صدور گواهی EV برای domain ها به درستی هویت و وجود قانونی را بررسی نکنند، اعتبار آن گواهی‌ها به خطر می‌افتد.

تیم گوگل کروم تحقیقات خود را از ۱۹ ژانویه آغاز کرد و دریافت که سیاست های صدور گواهی و اقدامات Symantec از چند سال گذشته غیرقابل اعتماد است و می‌تواند یکپارچگی سیستم TLS ای که برای احراز هویت ، امن نگه داشتن داده‌ها و اتصالات به اینترنت استفاده می شود را تهدید کند.

تحت این حرکت، تیم گوگل کروم مراحل زیر را به عنوان مجازات پیشنهاد کرده است:

۱ – گواهی‌های EV صادرشده توسط Symantec تا امروز، به گواهی‌های دامنه معتبرِ کمتر امن (less-secure domain validated certs-) تنزل رتبه می‌یابند. یعنی مرورگر کروم بلافاصله نمایش نام دارنده‌ی دامنه‌ی معتبر - validated domain- در نوار آدرس را برای مدت حداقل یک سال متوقف می‌کند.

۲ – برای محدود کردن ریسک هرگونه صدور اشتباهِ بیشتر، کلیه‌ی گواهی‌هایی که تازه صادر شده‌اند برای اینکه بتوانند مورد اعتماد گوگل کروم قرار بگیرند، نباید دوره‌ی اعتباری بیش از ۹ ماه داشته باشند. (از نسخه‌ی ۶۱ کروم این ویژگی فعال خواهد شد.)

۳ – گوگل یک بی‌اعتمادی افزایشی را پیشنهاد کرده: کاهش تدریجی »حداکثر عمر "گواهی‌های Symantec در دوره ی انتشار نسخه‌های متفاوت کروم، که آن‌ها را ملزم می‌کند تا گواهی‌ها را دوباره صادر و دوباره تایید کنند."

این یعنی، بعد از انتشار کروم ۶۴، که انتظار می‌رود در اوایل سال ۲۰۱۸ اتفاق بیفتد، مرورگر کروم تنها به گواهی‌های Symantec ای اعتماد خواهد کرد که برای ۹ ماه (۲۷۹ روز) یا کمتر صادر شده‌اند.

گوگل معتقد است که این حرکت تضمین می‌کند که توسعه‌دهندگان وب نسبت به ریسک بی‌اعتمادی آینده به گواهی های صادرشده توسط Symantec آگاه هستند .

پاسخ – Symantec ادعاهای گوگل "اغراق‌آمیز و گمراه‌کننده" است.

Symantec پاسخ داده و اظهار داشته است که ادعای گوگل مبنی بر صدور اشتباه ۳۰۰۰۰ گواهی SSl "اغراق آمیز و گمراه‌کننده" است.

"ما به شدت نسبت به اقدامی که گوگل برای هدف قرار دادن گواهی های SSL/TLS، Symantec انجام داده است اعتراض داریم. این اقدام غیرمنتظره بود، و ما معتقدیم که آن پستِ وبلاگ غیرمسئولانه بود."

"در حالی که همه‌ی CA های اصلی وقایع صدور اشتباهی گواهی SSL/TLS را تجربه کرده‌اند، گوگل تنها از گواهی مجاز Symantec در پروپوزال خود نام برده با اینکه واقعه‌ی صدور اشتباه گواهی ها که توسط پست وبلاگی گوگل شناسایی شده شامل چندین CA می‌شود."

گردآورنده: حسین علیمرادی

پچ آسیب پذیری وای فای iOS آپدیت شد.

اپل آپدیت اضطراری امنیتی را برای سیستم عامل ios خود منتشر کرده است تا یک آسیب پذیری جدی که wifi را تحت تاثیر قرار می دهد را کنترل کند.

با توجه به گزارش tech giant، این نقص یک stack-based buffer overflow است که به مهاجم اجازه می دهد هر کد دلخواهی را روی wifi chip اجرا کند.

این باگ امنیتی، با شناسه CVE-2017-6975، از طریقِ اعتبارسنجیِ ورودیِ بهبودیافته - improved input validation - به همراه انتشار ios 1.3.1 آمده است. این آپدیت برای آیفون ۵ و بعد از آن، آی پد لمسی نسل ۶ و بعد از آن، و آی پد نسل چهارم و بعد از آن در دسترس است.

9to5mac گزارش کرد در حالی که ios 10.3 پشتیبانی از دستگاه های ۳۲بیتی را قطع کرده است، آپدیتِ جدید پشتیبانی برای این سیستم ها را دوباره معرفی کرده است.

این آسیب پذیری توسط Gal Benamini از Google Project Zeroشناخته و گزارش شده است. Google Project Zero معمولا جزییات نقص هایی که توسط محققانش پیدا می شود را بعد از ۹۰ روز افشا می کند.

در راهنمای امنیتی که اپل ارائه کرده است، به کاربران خود توصیه کرده است که در صورت امکان این آپدیت را فورا نصب کنند و همچنین اشاره کرده است که این آپدیت تنها از طریق iTunes و Software Update utility بر رو دستگاه های ios در دسترس است؛ این آپدیت در سایت دانلودهای اپل - Apple Download Website - یا اپلیکیشن کامپیوتری Software Updateنشان داده نمی شود.

ios 10.3.1 تنها یک هفته پس از اینکه اپل دسترسی عمومی ios 10.3 را اعلام کرد، منتشر شد. ios 10.3 بسیاری از ویژگی ها و patch های جدید برای حدود ۹۰ آسیب پذیری را در بر دارد که در حدود ۳۰ تا از این باگ های امنیتی توسط محققان Google Project zero به اپل گزارش شده است.

گردآورنده: حسین علیمرادی

نقص وردپرس به هکرها اجازه‌ی تنظیم مجدد پسورد می‌دهد!

آسیب پذیری وردپرس ، مشهورترین سیستم مدیریت محتوا (CMS) در دنیا، به هکرهای راه دور اجازه می دهد تا تحت شرایط خاص پسورد کاربران هدف را مجدداً تنظیم کنند.

آسیب پذیری (CVE-2017-8295) حتی بعد از درک این موضوع که می تواند تمام ورژن های وردپرس شامل آخرین ورژن ۴.۷.۴ را تحت تاثیر قرار دهد خطرناک تر می شود.

نقص وردپرس در جولای سال گذشته توسط یک محقق لهستانی به نام Dawid Golunski که از هکرهای قانونی است کشف و به تیم امنیتی وردپرس گزارش شد ولیکن آنها تصمیم گرفتند این مساله را نادیده بگیرند و میلیون ها وب سایت را آسیب پذیر رها کنند.

"این مساله چندین بار به تیم امنیتی وردپرس گزارش داده شد و نخستین گزارش در جولای ۲۰۱۶ ارسال شد. این آسیب پذیری هم از طریق ایمیل امنیتی و هم از طریق وب سایت HackerOne گزارش شد" Golunski یک توصیه عمومی نوشت و درست زمانی که مشاهده کرد هیچ پیشرفتی در این مورد اتفاق نمی افتد بدون یک پچ رسمی آن را برای عموم منتشر کرد. Golunski همان محققی است که یک آسیب پذیری بسیار مهم را در کتابخانه متن باز PHPMailer کشف کرد که به هکرهای بدخواه اجازه می داد تا کد دلخواهی را در زمینه سرور اجرا کند و به اپلیکیشن تحت وب هدف لطمه بزنند.

این آسیب پذیری در شیوه ای که وردپرس درخواست تنظیم مجدد پسورد را پردازش می کند نهفته است.به طور کلی وقتی کاربری از طریق گزینه فراموش کردن پسورد، برای تنظیم مجدد پسورد درخواست می دهد ، وردپرس بلافاصله یک کد منحصربفرد را تولید و به ID ایمیل کاربر که در پایگاه داده ذخیره شده است ارسال می کند.

این آسیب پذیری چگونه است؟

در طول ارسال این ایمیل، وردپرس از متغیری به نام SERVER_NAME استفاده می کند تا نام میزبان سرور را بدست آورد و مقدار فیلدهای From/ Return-Path را تنظیم کند.

```
------[ wp-includes/pluggable.php ]------

...

if ( !isset( $from_email ) ) {
        // Get the site domain and get rid of www.
        $sitename = strtolower( $_SERVER['SERVER_NAME'] );
        if ( substr( $sitename, 0, 4 ) == 'www.' ) {
                $sitename = substr( $sitename, 4 );
        }

        $from_email = 'wordpress@' . $sitename;
}

...
```

در اینجا From به آدرس ایمیل فرستنده اشاره می کند و Return-Path به آدرس ایمیل جایی که ایمیل های bounce-back باید تحویل داده شود (در حالتی که به دلایلی تحویل ناموفق باشد) اشاره می کند.

طبق گفته Golunski یک هکر می تواند هم زمان با آغاز فرایند تنظیم مجدد پسورد برای کاربر ادمین، یک درخواست HTTP جعلی را با یک نام میزبان سفارشی (برای مثال attacker-mxserver.com) ارسال کند.

از آنجایی که نام میزبان در یک درخواست HTTP بدخواه ، دامنه تحت کنترل هکر، است فیلدهای Form و Return-Path در ایمیل تنظیم مجدد پسورد تصحیح می شود تا شامل یک ID ایمیل مربوط به دامنه هکر باشد برای مثال wordpress@attacker-mxserver.com به جای wordpress@victim-domain.com .

ادامه در صفحه بعد...

گردآورنده: حسین علیمرادی

نقص وردپرس به هکرها اجازه‌ی تنظیم مجدد پسورد می‌دهد! (ادامه...)

به دلیل هدر تصحیح شده HOST، SERVER_NAME به نام میزبان انتخابی توسط هکر تنظیم خواهد شد. در نتیجه وردپرس هدرها و بدنه ایمیل را به usr/bin/sendmail پاس خواهد داد.

توجه کنید که ایمیل تنظیم مجدد پسورد تنها به آدرس ایمیل قربانی تحویل داده خواهد شد اما از انجایی که حالا فیلدهای From و Return-Pathبه ID ایمیل هکر اشاره می کند ، هکر می تواند تحت سناریوهای زیر کد تنظیم مجدد را دریافت کند :

۱. اگر در این حالت قربانی به آن ایمیل پاسخ دهد ، به ID ایمیل هکر تحویل داده خواهد شد که شامل یک لینک تنظیم پسورد مجدد در تاریخچه پیام است.

۲. اگر به دلایلی، سرور ایمیل قربانی از کار بیفتد، ایمل تنظیم مجدد پسورد به طور خودکار به آدرس ذکر شده در فیلد Return-Path که به صندوق پستی هکر اشاره می کند می رود.

۳. در دیگر سناریوی ممکن ، هکر می تواند یک حمله DDoS به سرور ایمیل قربانی انجام دهد یا تعداد زیادی ایمیل ارسال کند به گونه ای که اکانت ایمیل قربانی نتواند برای مدتی پیامی دریافت کند و ایمیل bounce-back به فیلد Return-Path که به صندوق پستی هکر اشاره می کند می رود.

Golunski در یادداشتی در Hacker News بیان داشت : حمله The CVE-2017-8295 می تواند هم با تعامل کاربر (کاربر سناریوی پاسخ به ایمیل را مرتکب می شود) و یا بدون تعامل کاربر(پر شدن صندوق اسپم قربانی) انجام شود.حقیقت دیگری که باید ذکر شود این است که سواستفاده موفق از این نقص به این وابسته است که، حتی اگر وب سایت وردپرس دچار نقص باشد، همه وب سرورهای شامل WordPress میزبان شده روی هر سرور اشتراکی اجازه اصلاح نام میزبان از طریق هدر SERVER_NAME را داشته باشند.

هدر سرور SERVER_NAME می تواند روی پیکربندی پیش فرض وب سرور Apache با استفاده از هدر HOSTیک درخواست HTTP دستکاری شود.

به ادمین های وردپرس توصیه شده است تا پیکربندی سرورشان را به روزرسانی کنند تا UseCanonicalName را قادر سازند تا مقدار ازپیش تعیین شده یا ثابت SERVER_NAME را تقویت کند.

گردآورنده: حسین علیمرادی

مخاطرات امنیتی مهم محصولات مایکروسافت در سال ۲۰۱۷ و بسته به روزرسانی مربوطه

ID	شماره به روز رسانی	به روز رسانی	خلاصه	نرم افزار
MS17-001	۳۲۱۴۲۸۸	Security Update for Microsoft Edge	یک آسیب پذیری امنیتی در Microsoft Edge است و می تواند حقوق دسترسی را در صورت مشاهده یک صفحه خاص افزایش دهد. مهاجمی که موفق به بهره برداری از این آسیب پذیری شود مجوز بالایی را در دایرکتوری فضا نام یک سیستم آسیب پذیر به دست می آورد.	Microsoft Windows, Microsoft Edge
MS17-002	۳۲۱۴۲۹۱	Security Update for Microsoft Office	یک آسیب پذیری امنیتی در Microsoft Office است و می تواند یک قطعه کد دستکاری شده را از راه دور اجرا کند. مهاجمی که موفق به بهره برداری از این آسیب پذیری شود می تواند یک کد دلخواه را در زمینه سیستم آسیب دیده اجرا کند. کاربران با حقوق دسترسی محدودتر در سیستم کم تر در معرض این آسیب قرار دارند.	Microsoft Office, Microsoft Office Services and Web Apps
MS17-003	۳۲۱۴۶۲۸	Security Update for Adobe Flash Player	یک آسیب پذیری امنیتی در Adobe Flash Player برای تمامی نسخه های ویندوز ۸.۱، ویندوز سرور ۲۰۱۲، ویندوز سرور ۲۰۱۲ R2، ویندوز ۸.۱ RT، ویندوز ۱۰ و ویندوز سرور ۲۰۱۶ است.	Microsoft Windows, Adobe Flash Player
MS17-004	۳۲۱۶۷۷۱	Security Update for Local Security Authority Subsystem Service	یک آسیب پذیری امنیتی در خدمت رسانی زیرسیستم امنیتی تشخیص هویت محلی (LSASS) است. مهاجمی که موفق به بهره برداری از این آسیب پذیری می شود می تواند یک انسداد سرویس در خدمات LSASS ایجاد کند و باعث راه اندازی مجدد و خودکار سیستم هدف شود.	Microsoft Windows
MS17-005	۴۰۱۰۲۵۰	Security Update for Adobe Flash Player	یک آسیب پذیری امنیتی در Adobe Flash Player برای تمامی نسخه های ویندوز ۸.۱، ویندوز سرور ۲۰۱۲، ویندوز سرور ۲۰۱۲ R2، ویندوز ۸.۱ RT، ویندوز ۱۰ و ویندوز سرور ۲۰۱۶ است.	Microsoft Windows, Adobe Flash Player

گردآورنده: امین زمانی

مخاطرات امنیتی مهم محصولات مایکروسافت در سال ۲۰۱۷ و بسته به روزرسانی مربوطه (ادامه...)

ID	شماره به روز رسانی	به روز رسانی	خلاصه	نرم افزار
MS17-006	۴۰۱۳۰۷۳	Cumulative Security Update for Internet Explorer	یک آسیب پذیری در مرورگر Internet Explorer است که می تواند اجازه اجرای کد از راه دور را به یک کاربر مشاهده کننده یک صفحه وب خاص با استفاده از Internet Explorer بدهد. مهاجمی که موفق به بهره برداری از این آسیب پذیری شود به حقوق دسترسی مشابه همان کاربر دست پیدا می کند. اگر کاربر جاری دارای حقوق دسترسی مدیریتی باشد، مهاجم با موفقیت کنترل کامل سیستم آسیب دیده را به دست می گیرد. یک مهاجم می تواند اعمالی چون نصب برنامه، مشاهده، تغییر یا حذف داده ها و ایجاد یک حساب کاربری جدید با حقوق دسترسی کامل را انجام دهد.	Microsoft Windows, Microsoft Internet Explorer
MS17-007	۴۰۱۳۰۷۱	Cumulative Security Update for Microsoft Edge	یک آسیب پذیری در مرورگر Microsoft Edgeاست که می تواند اجازه اجرای کد از راه دور را به یک کاربر مشاهده کننده یک صفحه وب خاص با استفاده از Microsoft Edgeبدهد. مهاجمی که موفق به بهره برداری از این آسیب پذیری شود می تواند کنترل کامل به سیستم آسیب دیده داشته باشد و اعمالی چون نصب برنامه، مشاهده، تغییر یا حذف داده ها و ایجاد یک حساب کاربری جدید با حقوق دسترسی کامل را انجام دهد.	Microsoft Windows, Microsoft Edge
MS17-008	۴۰۱۳۰۸۲	Security Update for Windows Hyper-V	یک آسیب پذیری در سیستم عامل ویندوز است که به یک کاربر میهمان در سیستم عامل ویندوز بر روی Hyper-V اجازه اجرای کدهای دلخواه را می دهد. کسانی که نقش های Hyper-V را فعال نکرده اند از این آسیب پذیری در امان هستند.	Microsoft Windows
MS17-009	۴۰۱۰۳۱۹	Security Update for Microsoft Windows PDF Library	یک آسیب پذیری در سیستم عامل ویندوز است که اجازه اجرای کد بر روی سیستم عامل کاربرانی را می دهد که اسناد PDF را به صورت آنلاین مشاهده می کنند یا یک سند دستکاری شده را باز می کنند.	Microsoft Windows

گردآورنده: امین زمانی

مخاطرات امنیتی مهم محصولات مایکروسافت در سال ۲۰۱۷ و بسته به روزرسانی مربوطه (ادامه...)

نرم افزار	خلاصه	به روز رسانی	شماره به روز رسانی	ID
Microsoft Windows	یک آسیب پذیری در سیستم عامل ویندوز است که به یک مهاجم اجازه ارسال یک پیام دستکاری شده خاص به سرور SMBv1 از راه دور را می دهد.	Security Update for Microsoft Windows SMB Server	۴۰۱۳۳۸۹	MS17-010
Microsoft Windows	یک آسیب پذیری در Uniscribe است که اجازه اجرای کد بر روی سیستم عامل کاربرانی را می دهد که یک وب سایت خاص یا یک سند خاص را باز می کنند. کاربرانی که حقوق دسترسی کم تری دارند نسبت به کاربرانی با حقوق دسترسی مدیریتی، کم تر آسیب پذیر هستند.	Security Update for Microsoft Uniscribe	۴۰۱۳۰۷۶	MS17-011
Microsoft Windows	یک آسیب پذیری در سیستم عامل ویندوز است که اجازه اجرای کد بر روی سیستم عامل کاربرانی را می دهد که یک برنامه خاص متصل به سرور iSNS را اجرا می کنند. برای اجرای برنامه درخواست های مخرب به سرور ارسال می شود.	Security Update for Microsoft Windows	۴۰۱۳۰۷۸	MS17-012
Microsoft Windows Microsoft Office, Skype for Business, Microsoft Lync, Microsoft Silverlight	یک آسیب پذیری در سیستم عامل ویندوز، Microsoft Office، Skype for Business، Lync و Silverlightاست که اجازه اجرای کد بر روی سیستم عامل کاربرانی را می دهد که یک وب سایت خاص یا یک سند خاص را باز می کنند. کاربرانی که حقوق دسترسی کم تری بر روی سیستم عامل دارند نسبت به کاربرانی با حقوق دسترسی مدیریتی، کم تر آسیب پذیر هستند.	Security Update for Microsoft Graphics Component	۴۰۱۳۰۷۵	MS17-013
Microsoft Office, Microsoft Office Services and Web Apps, Microsoft Server Software, Microsoft Communications Platforms and Software	یک آسیب پذیری در Microsoft Officeاست که اجازه اجرای کد بر روی سیستم عامل کاربرانی را می دهد که اسناد دستکاری شده و خاصی از آفیس را باز می کنند. کاربرانی که حقوق دسترسی کم تری بر روی سیستم عامل دارند نسبت به کاربرانی با حقوق دسترسی مدیریتی، کم تر آسیب پذیر هستند.	Security Update for Microsoft Office	۴۰۱۳۲۴۱	MS17-014

گردآورنده: امین زمانی

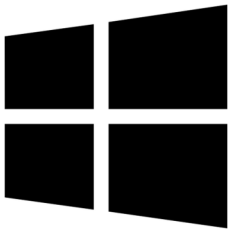
مخاطرات امنیتی مهم محصولات مایکروسافت در سال ۲۰۱۷ و بسته به روزرسانی مربوطه (ادامه...)

نرم افزار	خلاصه	به روز رسانی	شماره به روز رسانی	ID
Microsoft Exchange	یک آسیب پذیری در Microsoft Exchangeاست که اجازه اجرای کد بر روی سرور Microsoft Exchangeرا می دهد اگر یک مهاجم، یک ایمیل با پیوست مخرب ارسال کند.	Security Update for Microsoft Exchange Server	۴۰۱۳۲۴۲	MS17-015
Microsoft Windows	یک آسیب پذیری در IIS است. این آسیب پذیری می تواند حقوق دسترسی را ارتقاء دهد اگر یک کاربر به یک URL خاص مراجعه کند که توسط یک سرور IISآسیب دیده پشتیبانی می شود. مهاجمی که موفق به بهره برداری از این آسیب پذیری شود می تواند اسکریپت هایی را برای به دست آوردن برخی اطلاعات در مرورگر کاربر اجرا کند.	Security Update for Windows IIS	۴۰۱۳۰۷۴	MS17-016
Microsoft Windows	یک آسیب پذیری در سیستم عامل ویندوز است و می تواند حقوق دسترسی را ارتقاء دهد اگر یک مهاجم یک برنامه خاص را بر روی سیستم عامل هدف اجرا کند.	Security Update for Windows Kernel	۴۰۱۳۰۸۱	MS17-017
Microsoft Windows	یک آسیب پذیری در سیستم عامل ویندوز و می تواند حقوق دسترسی را ارتقاء دهد و کنترل سیستم را در اختیار بگیرد اگر یک مهاجم یک برنامه خاص را بر روی سیستم عامل هدف اجرا کند.	Security Update for Windows Kernel-Mode Drivers	۴۰۱۳۰۸۳	MS17-018
Microsoft Windows	یک آسیب پذیری در ADFS است. این آسیب پذیری می تواند اطلاعات کاربر را افشاء کند. اگر یک مهاجم یک درخواست خاص به یک سرور ADFS بفرستد به اطلاعاتی حساس در مورد سیستم هدف دسترسی پیدا می کند.	Security Update for Active Directory Federation Services	۴۰۱۰۳۲۰	MS17-019

گردآورنده: امین زمانی

مخاطرات امنیتی مهم محصولات مایکروسافت در سال ۲۰۱۷ و بسته به روزرسانی مربوطه (ادامه...)

نرم افزار	خلاصه	به روز رسانی	شماره به روز رسانی	ID
Microsoft Windows	یک آسیب پذیری در DVD Maker است. این آسیب پذیری به مهاجمان اجازه دسترسی به اطلاعات حساس در مورد سیستم هدف را می دهد.	Security Update for Windows DVD Maker	۳۲۰۸۲۲۳	MS17-020
Microsoft Windows	یک آسیب پذیری در سیستم عامل ویندوز است و می تواند اطلاعات کاربر را افشاء کند اگر DirectShowمحتوای دستکاری شده خاصی را که بر روی یک وب سایت مخرب میزبانی می شود باز کند. مهاجمی که موفق به بهره برداری از این آسیب پذیری شود می تواند سیستم هدف را کنترل کند.	Security Update for Windows DirectShow	۴۰۱۰۳۱۸	MS17-021
Microsoft Windows	یک آسیب پذیری در سیستم عامل ویندوز است و و می تواند اطلاعات کاربر را افشاء کند اگر یک کاربر به یک صفحه وب سایت مخرب مراجعه کند. با این حال، در تمام موارد مهاجم باید کاربر هدف را متقاعد به رجوع به یک لینک خاص بکند که به طور معمول از طریق یک ایمیل یا پیام رسان انجام می شود.	Security Update for Microsoft XML Core Services	۴۰۱۰۳۲۱	MS17-022
Microsoft Windows, Adobe Flash Player	یک آسیب پذیری امنیتی در Adobe Flash Player برای تمامی نسخه های ویندوز ۸.۱، ویندوز سرور ۲۰۱۲، ویندوز سرور ۲۰۱۲ R2، ویندوز ۸.۱ RT، ویندوز ۱۰ و ویندوز سرور ۲۰۱۶ است.	Security Update for Adobe Flash Player	۴۰۱۴۳۲۹	MS17-023



گردآورنده: امین زمانی

حملات فیشینگ از طریق گوگل

گوگل مشکل را در کمتر از یک ساعت از زمان اعلام آن توسط برنامه حل کرده است.

این شرکت در این باره میگوید:

ما توانستیم این نبرد را تقریباً در یک ساعت خاتمه دهیم در حالی که اطلاعات تماس در دسترس بودند و برای نبرد استفاده می‌شدند. تحقیقات ما نشان میدهد که هیچ تاریخ دیگری در معرض دید نبوده است.

همچنین گوگل اعلام کرد که فقط ۰/۱ درصد از کاربران تحت تأثیر حملات فیشینگ بوده‌اند.

اما فوربس اشاره کرد که اگر تعداد کاربران جیمیل دقیق باشد بیش از یک میلیون کاربر در دام این کلاهبرداری افتاده اند.

حالا به اصل ماجرا می پردازیم:

رسانه‌های زیادی گزارش دادند که توسط یک طرح ماهرانه فیشینگ هرنامه دریافت کرده‌اند. کلاه برداران از طریق شبیه سازی نرم‌افزار اسناد گوگل به جمع آوری اطلاعات تماس و شماره های شما اقدام میکنند. یک ایمیل شما را به ویرایش یک سند در نرم‌افزار اسناد گوگل دعوت میکند. لینک موجود در ایمیل تا حدی مشکوک است. انگار که یک کاربر ردیت قربانی را ترغیب به چیزی کند.

اما هنوز هم مبنای گوگل بر این است که شما با کلیک بر روی یک لینک به صفحه واقعی ورود گوگل هدایت شوید تا بتوانید با انتخاب حساب کاربری وارد نرم‌افزار اسناد گوگل شوید. این کار شما را متوجه می کند که با ورود به نرم‌افزار اسناد گوگل در دام کلاه‌بردار افتاده اید. وقتی شما روی لینک کلیک می کنید از شما خواسته می‌شود تا به نرم‌افزار اسناد گوگل اجازه خواندن، ارسال، حذف و مدیریت ایمیل و مدیریت تماس های تان را بدهید. با انجام این کار شما به یک غریبه خطرناک مجوز دسترسی داده‌اید.

در برداشت اول ظاهراً برنامه ای به نام نرم‌افزار اسناد گوگل از شما درخواست مجوز کرده است. در نتیجه شما به صفحه ورود

واقعی گوگل منتقل می‌شوید اما باید به آدرس url دقت کنید و به سادگی از آن نگذرید. تنها سرنخی که وجود دارد آدرس ایمیلی است که مربوط به توسعه دهنده برنامه جعلی است.

جیم استریم در ردیت گفته است که اگر روی لینک اسناد گوگل کلیک کنید به شما نشان خواهد داد که درواقع این ایمیل ها بصورت اتفاقی از طریق حساب‌های جیمیل منتشر می‌شوند و ممکن است صاحب آن حسابی که از طرف او ایمیل برای شما ارسال شده دسترسی کامل به ایمیل شما پیدا کند.

مشخص نیست این کلاهبرداری تا چه حدگسترش یافته است. اما این موضوع در همه جای اینترنت افکار را به خود مشغول کرده است که چند نفر این ایمیل را دریافت کرده اند.

گوگل در توییتر اعلام کرد که به وسیله غیرفعال کردن حساب‌های متخلف، حذف صفحات تقلبی و بروزرسانی توسط مرور امن این موقعیت را تحت کنترل دارد.

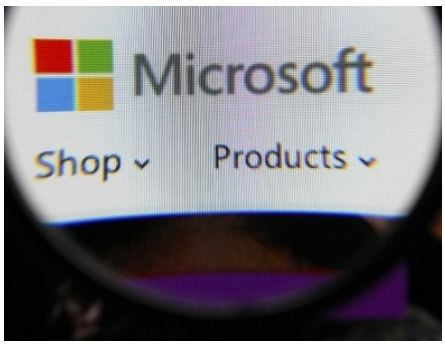
اگر این اتفاق برای شما هم افتاده، به صفحه سایتها و برنامه‌های متصل در گوگل بروید و دسترسی های برنامه‌ای به نام نرم‌افزار اسناد گوگل را حذف کنید. ضمناً در مورد ایمیل‌هایی که اسناد گوگل را با شما به اشتراک میگذارند مراقب باشید، حتی اگر از طرف یک ایمیل آشنا باشد. ابتدا بررسی کنید و مطمئن شوید که چه کسی آن را ارسال کرده است.

گردآورنده: محسن یزدی نژاد

پچ های حملات zero day که توسط هکرهای روسی مورد سو استفاده قرار گرفته شده بودند!

به روزرسانی های پچ شرکت مایکروسافت در ماه می، دهها آسیب پذیری که توسط مجرمان رایانه ای سودجو و دو گروه جاسوسی وابسته به روسیه مورد سواستفاده قرار گرفته بودند را مورد توجه قرار داد. ماکروسافت بیش از ۵۰ چاله امنیتی که ویندوز، اینترنت اکسپلورر، Edge، Office ، NET framework. و فلش پلیر منتشر شده توسط ادوپ را تحت تاثیر قرار می داد را برطرف کرد. ماکروسافت در پستی فاش کرد که این شرکت برای حفاظت از مشتریانش در برابر مهاجمانی که از آسیب پذیری های فیلتر Encapsulated PostScript (EPS) آفیس بهره می برند با ESET و FireEye همکاری می کند. هر دو شرکت ESET و FireEye گزارش هایی را از حملات مشاهده شده ، منتشر کردند. FireEye حملاتی را مشخص کرد که توسط دو گروه جاسوسی وابسته به دولت روسیه و یک شخص ناشناس با انگیزه مالی انجام شده بود. طبق گفته این شرکت امنیتی گروهی موسوم به Turla، Waterbug، KRYPTON و Venomous Bear از یک آسیب پذیری اجرای کد راه دور (REC) آفیس موسوم به CVE-2017-0261 استفاده کرده اند تا یک پیوند(ایمپلنت) جاوااسکریپت سفارشی که لقب SHIRIME را به آن داده اند پخش کند. این آسیب پذیری همچنین در سال های گذشته توسط مجرمان رایانه ای سودجو استفاده شده تا نوع جدیدی از بدافزارِ NETWIRE را پخش کند.

گروه Turla در حملات خود از CVE-2017-0001 برای افزایش سطح دسترسی (privilege escalation) استفاده کرده اند در حالی که مجرمان رایانه ای از CVE 2016-7255-برای افزایش سطح دسترسی بهره جسته اند.



FireEye و ESET حملاتی را مشاهده کرده اند که با آسیب پذیری روز صفر سروکار دارند و توسط گروه هایی به نام های APT28 ، Pawn Storm ، Fancy Bear ، Sofacy ، Sednit و Strontium انجام شده است.این گروه وابسته به روسیه که بعضی عقیده دارند که در حملات سایبری انتخابات فرانسه دست دارند از یک نقص RECآفیس (CVE-2017-0262) و افزایش سطح دسترسی ویندوز (CVE-2017-0263) بهره جسته اند. این دو شرکت امنیتی ردیابی کرده اند که بدافزار پخش شده در این حملات Seduploader و GAMEFISH هستند.

ماکروسافت اشاره کرد که حملات Turla در ماه مارس مشخص شدند و مشتریانی که سیستم های به روز دارند از اوایل آن ماه که CVE-2017-0001 اصلاح شد در امنیت هستند. در آوریل نیز این شرکت حفاظتی را طراحی کرد که در آن به طور پیش فرض فیلتر EPS غیرفعال است تا از حملات EPS جلوگیری کند. به روزرسانی های منتشر شده در این ماه آسیب پذیری های مربوط به EPS در آفیس(CVE-2017-0261 و CVE-) 2017-0262 را اصلاح کرد تا مشتریانی که نیاز به استفاده از فیلترهای EPS دارند اطمینان یابند که در امنیت هستند.

دیگر zero day اصلاح شده توسط ماکروسافت یعنی CVE-2017-0222 موجب نشست حافظه در اینترنت اکسپلورر است که می تواند برای اجرای راه دور کد استفاده شود. اطلاعاتی درباره نحوه استفاده مهاجمان از این نقص منتشر نشده است.

این شرکت چهار آسیب پذیری فاش شده دیگر را نیز مورد توجه قرار دارد که شامل موارد زیر است : نقص RES در موتورهای جاوا اسکریپت مرورگرهای وب (CVE-2017-0229)، یک افزایش سطح دسترسی در CVE-2017-0241 (Edge) ، دور زدن هشدارهای محتوای ترکیبی در اینترنت اکسپلورر (CVE-2017-0064) و یک آسب پذیری جعل فیلترِ اسمارت اسکرین مرورگر (CVE-2017-0231).

گردآورنده: حسین علیمرادی

تبلیغات فلش پلیری تقلبی در اسکایپ

کاربران زیادی هفته ی گذشته در توییتر با نشان دادن عکس هایی از صفحه نمایش خود ، گزارش دادند که اسکایپ ،آنها را مجبور به دانلود نسخه بروز شده ی فلش پلیر کرده است. با تأکید بر اسم فایل نصب شده بنام FlashPlayer.hta، بروزرسانی جعلی ای یافت شد که توسط یکی از تبلیغات درون-برنامه ای بکار گرفته شده که معمولا این برنامه‌ی پیام رسان به کاربرانش ارائه میدهد.

فایل HTA که درواقع یک فایل HTML است، از طریق چیزی که یک کاربر به آن مراجعه‌کرده است مثل سایتی با "ظاهر عاری از جزئیات" بخدمت گرفته شده و چنین باوری درمورش وجود دارد که این فایل برای دانلود یک باج افزار یا انواع بدافزارهای دیگر طراحی شده است. (HTA برای توزیع باج افزارهایی مانند Locky، Cerber و اخیرا Spora پدیدار شده است).

BleepingComputer گزارش میدهد این بسته ی فایل طوری طراحی شده تا کد جاوااسکریپتی را دچار سردرگمی کند. این کد برای نمایش و اجرای یک پاورشل اسکریپتی که موظف است محتوای مرحله دوم را دانلود کند که در یک مورد یک فایل JSE (جاوااسکریپت رمزگذاری شده) بود طراحی شده است . گرچه به این خاطر که دامنه هایی که میزبان محتوا هستند، حین تجزیه تحلیلها از کارافتاده بود، محققین مشغول بررسی حادثه، نتوانستند تأیید کنند که چه نوع بدافزاری پخش شده است.

صرف نظر از اینکه آنها توانستند دو دامنه oyomakaomojiya.org و cievubeataporn.net را به دهها دامنه مشکوک دیگر متصل کنند، بیشتر آنها قبلا شریک انواع مختلف فعالیتهای مخرب شده بودند. تمام دامنه هایی که تنها با استفاده از دو آدرس ایمیل ثبت شده اند ولی بنظر میرسد که هیچکدام قبل از تاریخ ۲۲ فوریه ۲۰۱۷ ثبت نشده اند.

بعلاوه، تعدادی از آدرسهای IP میزبان سایتها، با سرورهایی شریک شده‌اند که قبلا میزبان دامنه های مخرب دیگر بوده اند. با نفوذ بیشتر به عمق مسئله، محققین دریافتند تاکنون یک آدرس ایمیل دیگر برای ثبت بیش از ۳۵ دامنه از ۲۳ فوریه ۲۰۱۷ استفاده شده است و به این نتیجه رسیدند که گروهی از هکرهای ماهر روزانه اقدام به ثبت تعداد زیادی دامنه جدید میکردند، که بیشتر شبیه به بخشی از یک لشکرکشی بدافزاری است.

به این خاطر که مهاجمان از تعداد زیادی دامنه که بیشتر آنها TTL کوتاهی داشتند استفاده میکردند، محققین نتوانستند محتوای نهایی را نگهدارند.

هنوز هم واضح نیست که چطور تبلیغات مخرب توسط اسکایپ به خدمت گرفته شدند (گرچه اتفاقات مشابه قبلا دیده شده است)، اما محتمل ترین دلیل این است که مجرمین سایبری بوسیله تظاهرهای دروغین، اقدام به ثبت تبلیغ با شبکه تبلیغات کردند و سپس کد مخرب خود را بجای تبلیغات قانونی ارائه کردند.

مایکروسافت به درخواست برای اطلاعات بیشتر درمورد این اتفاق، پاسخی نشان نداد.

طبق گزارش ژانویه ۲۰۱۷ از RiskIQ، پدیده بدافزار کردن، از سال۲۰۱۶ تاکنون، ۱۳۲٪ افزایش داشته است

گردآورنده: حسین علیمرادی

پشت پرده‌ی WannaCry

از زمان ورود باج افزار WannaCry محققان نتوانستند که نیروی پشتیبان این حملات را تشیخص دهند. بررسی های جدید توسط Flashpoint نشان می دهد که احتمال زیادی بین وابستگی هکرهای چینی با باج افزار WannaCry موجود است. یک شرکت مربوط به انجام خدمات زبانشناسی با بررسی برروی نوشته ها و هشدارهای موجود در این باج افزار به نتایج جالبی دست یافت.

چیزهایی وجود دارند که ما با اطمینان در خصوص باج افزار WannaCry میدانیم. این باج افزار توسط مجرمین اینترنتی و با استفاده از بخشی از exploit مربوط به NASA که توسط گروه Shadow Brokers نشر یافته است کار می کند. این باج افزار برروی صدها کامپیوتری که با سیستم عامل ویندوز ۷، ویستا و XP کار می کنند قابل اجرا می باشد.

ممکن است که ما در خصوص سازندگان این باج افزار که اطلاعات کامپیوترهای کاربران را رمزگذاری می کنند اطلاعات دقیقی نداشته باشیم. اما تحقیقات اخیر از شرکت امنیتی Flashpoint مشخص کرده است که انگشت اتهام به سمت چینی ها خواهد بود.

در یک پست وبلاگ، Flashpoint لیستی از نتایج بررسی های زبان شناسی برروی پیغام های باج افزار WannaCry را ارئه نموده است. این تیم متن های موجود در این باج افزار را بر اساس محتوا، دقت و استایل بررسی کرده است.

Flashpoint دریافته است که نمونه های زبان های مختلف موجود در این باج افزار یک فایل پیکربندی با ترجمه های مختلف به سایر زبان ها دارد. همچنین متوجه شده اند که تقریبا تمامی نوشته ها با مترجم گوگل به سایر زبان ها ترجمه شده است به غیر از نوشته های چینی و انگلیسی که توسط یک انسان نوشته شده اند. همچنین مشخص شده است که متن انگلیسی به عنوان متن مرجع برای ترجمه به سایر زبان های دنیا مورد استفاده قرار گرفته است.

اما متن چینی هشدار موجود در این باج افزار از لحاظ فرمت، محتوا و قالب با سایر زبان ها متفاوت است. همچنین احتمال استفاده از مترجم گوگل نیز در ترجمه ی چینی به انگلیسی و انگلیسی به چینی در این بررسی رد شد.

بررسی ها حاکی از آن است که برخی از کاراکترهای موجود در متن به زبان چینی منحصر به فرد است که این امر نشان دهنده ی این است که این متون توسط افراد خبره چینی نوشته شده است. ویژگی های تایپی آن نشان دهنده ی این امر است که متن نوشته شده توسط یک سیستم با کیبورد ورودی چینی نوشته شده است. همچنین در متن چینی، از گرامر، حروف گذاری و انتخاب واژگان به درستی استفاده شده است.

متن موجود محدود به چینی زبانان جنوب چین می باشد. یک شاخص برای این تشخیص میزان بسط جملات در متن انگلیسی می باشد.

Flashpoint در حالی که احتمال داد این باج افزار مربوط به نیروهای کشور چین می باشد اعلام نمود که اشاره به نکات گمراه کننده عمدی در این متون را نباید فراموش کرد.

گردآورنده: محمد مرتضوی

مخفی کردن سرور کنترل در اکانت اینستاگرام Britney Spears

اگر میخواهید دستورات خود را برای کنترل سرورهایتان مخفی کنید کافیست این دستورات را در اینستاگرام پست کنید.

بله، عنوان خبر را درست خواندید. طبق گزارش Ars Technica، هکرهای روسی Turla یک راه منحصر و یکتا برای ایجاد ارتباط ایمن بین دستورات و سرور کنترل یافته اند. این کار به وسیله ی ارسال دستورات برروی پست های مربوط به صفحه ی Britney انجام می شود. دستورات مربوط به هدایت بد افزار و لینک اتصال به سرور کنترل عناوینی هستند که عموما بدافزارها با آنان ارتباط برقرار می کنند تا دستورات مورد نیاز را دریافت نمایند و داده هایی از قربانی را بدزدند. در ظاهر ایجاد یک C&C سرور کار ساده ای به نظر می رسد اما در اصل این کار یک مشکل بزرگ و اساسی برای سازندگان بدافزارها می باشد.

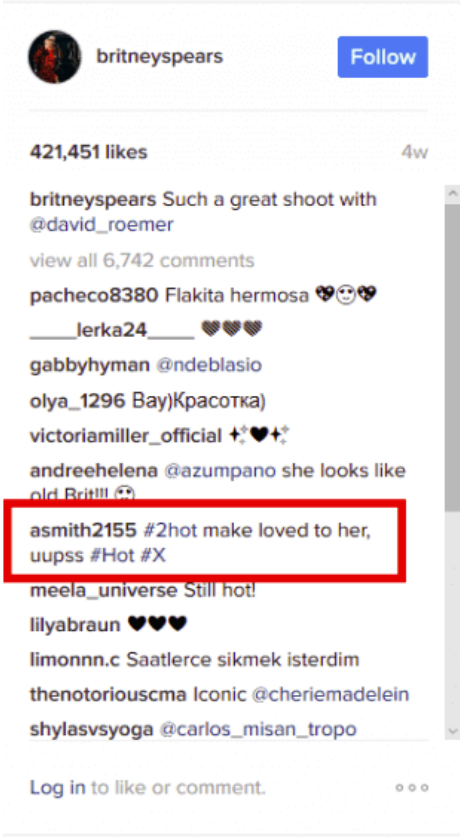
برای بدافزارها باید مشخص باشد که با چه سروری ارتباط برقرار نمایند. استفاده از آدرس سرور در کد بد افزارها عمل خوبی محسوب نمی شود. از طرفی هم با بررسی ها امنیتی به راحتی می توان به کد بد افزار دست پیدا کرد و آدرس سرور را استخراج نمود و ارتباط با سرور را مسدود کرد. این دقیقا مشابه کاریست که برای توقف باج افزار WannaCry مورد استفاده قرار گرفت.

برای اطمینان از این که بدافزار بداند با چه سروری در ارتباط است و شخص دیگری از خود بدافزار به این موضوع پی نبرد، گروه Turla یک راه ساده و ارزشمند را برای مشخص کردن مکان سرور کنترل پیاده سازی نمود. آن ها آدرس سرور کنترل را در یک کامنت در پست های موجود در اینستاگرام قرار دادند. بدافزار این کامنت ها را بررسی و آنان را هش (Hash) می نماید تا یک مقدار قابل قبول پیدا نماید. سپس به راحتی و با استفاده از عبارات منظم در ریاضیات برروی کامنت های به راحتی لینک C&C به دست خواهد آمد.

از آن جایی که لینک سرور به طور مستقیم در کد برنامه و یا در کامنت ها موجود نیست. تشخیص این امر بسیار دشوار خواهد بود. کامنت واقعی در این سوال به صورت زیر بود

#۲Hot make loved to her, #uupss #Hot #X

و شامل کاراکترهای یونیکد غیر قابل چاپ برای کمک به ساخت لینک سرور کنترل می کند.



گردآورنده: محمد مرتضوی

Kharazmi CERT Coordinator Center

مرکز آپا دانشگاه خوارزمی

نشانی:

کرج - دانشگاه خوارزمی - کتابخانه‌ی مرکزی - طبقه‌ی همکف - مرکز آپا

رییس مرکز:

دکتر امید مهدی عبادتی

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

اعضای هیات علمی:

دکتر احسان ملکیان

دکتر امید مهدی عبادتی

وب سایت:

http://cert.khu.ac.ir/

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

محسن یزدی نژاد