سراج

۲۴ مهر ۱۳۹۵

شماره ۸۲

خبرنامه کارشناسی

اخبار فناوری اطلاعات و ارتباطات

مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج

هفته نامه | شماره هشتاد و nوم | سال دوم | ۱۰۴ صفحه

Expert Bulletin News

Information Communication Technology

2th year 2016 | Weekly bulletin

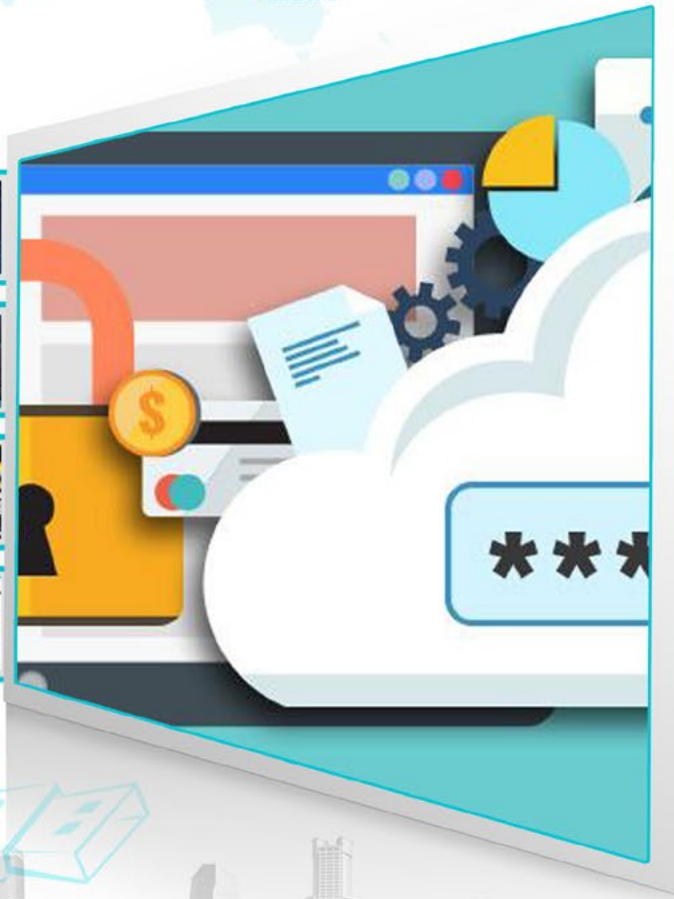
در این شماره می‌خوانید:

مسنجر فیس‌بوک از روش رمزگذاری واتس‌اپ استفاده می‌کند

بی‌اعتمادی شهروندان انگلیسی به مسئولان دولتی در زمینه‌ی حفاظت از اطلاعات

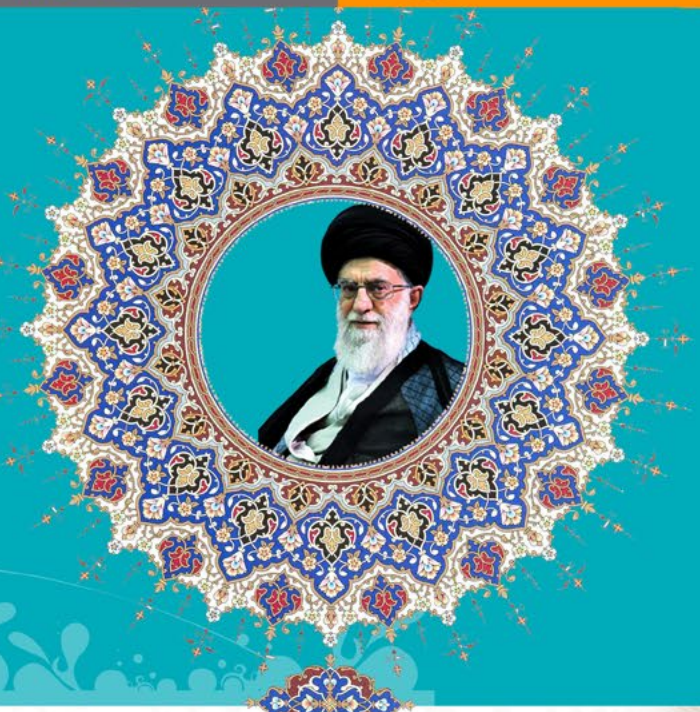
مدیر آژانس بین‌المللی انرژی اتمی از یک نفوذ سایبری به نیروگاه‌های هسته‌ای خبر داد

وصله آسیب‌پذیری منع سرویس در اندروید از سوی گوگل



بسم الله الرحمن الرحیم

آگاهی و بصیرت



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

مقام معظم رهبری (مد ظله العالی)

فهرست مطالب

فصل اول: اخبار عمومی

Pirate Bay، در فهرست وب‌گاه‌های مخرب تورنت. ۷
انتشار لیبره‌آفیس ۵.۳ در فوریه‌ی ۲۰۱۷. . . . . ۸
مسنجر فیس‌بوک از روش رمزگذاری واتس‌اپ استفاده می‌کند. ۹
درخواست از کاربران اوبونتو و Systemd برای به‌روزرسانی لینوکس. ۱۰
غیرفعال شدن ویژگی ارسال مجدد رایانامه‌ی یاهو کار را ۱۲
برای ترک این سرویس سخت‌تر می‌کند
سرویس پانورامیوی گوگل تعطیل خواهد شد. ۱۴
آیا در جست‌وجوی بهترین ابزارهای رمزنگاری هستید؟. ۱۶
آیا می‌خواهید از به‌روزرسانی خودکار به macOS Sierra نجات پیدا کنید؟. ۱۸
اپل مرور خصوصی Safari در iOS 10 را تضعیف کرد!. ۲۰
سرویس Spotify قربانیان را در دام حملات تبلیغاتی می‌اندازد!. ۲۲
به دنبال «طوفان متیو»، رایانامه‌های مخرب این طوفان نیز در راه است!.. . . . ۲۴
یک ابزار رایگان از کاربران مک در برابر نظارت وب‌کم حفاظت می‌کند!. ۲۵

فصل دوم: مدیریت امنیت

بی‌اعتمادی شهروندان انگلیسی به مسئولان دولتی در ۲۸
زمینه‌ی حفاظت از اطلاعات
بازداشت عاملان نفوذ به جی‌پی‌مورگان در مسکو. ۲۹
دومین نفوذ به بانک‌های متصل به سوئیفت ۳۱
پلیس لندن عاملان ورود بدافزار به ATMها را بازداشت کرد.. . . . . ۳۲
برنده‌ی جایزه‌ی ۵۰هزار دلاری برای ارائه‌ی راه حل یافتن ۳۳
دستگاه‌های آسیب‌پذیر IoT باشید
محکومیت دو عضو گروه Dridex به ۱۲ سال زندان.. . . . . ۳۵
سرقت اطلاعات مربوط به ۵۸ میلیون کاربر در یک ارائه‌دهنده ۳۶
خدمات ذخیره‌سازی
3 اولویت مهم در امنیت اطلاعات. ۳۸
آمازون در اقدام پیشگیرانه‌ای گذرواژه‌ی مشتریان را بازنشانی می‌کند.. . . . . ۴۰
مرکز صدور گواهی WoSign، بدنبال بخشیده شدن توسط مرورگرها. ۴۱

فصل سوم: سیاست سایبری

مدیر آژانس بین‌المللی انرژی اتمی از یک نفوذ سایبری ۴۳
به نیروگاه‌های هسته‌ای خبر داد
کشف یک در پشتی که رمزگذاری دیفی-هلمن صدها میلیون ۴۴
پیام را تهدید می‌کند

فهرست مطالب

کمک چند میلیون دلاری سنگاپور برای بهبود امنیت اطلاعات آسه‌آن ۴۵
مراکز تماس هندی ۷۵ میلیون دلار را با فریب شهروندان آمریکایی به چنگ آوردند ۴۶
بنیان‌گذار ویکی‌لیکس به قول خود عمل کرد ۴۷
ساخت ابزار سری یاهو برای پویش محتوای رایانامه‌ها به دستور آژانس امنیت ملی آمریکا ۴۹
FBI خواستار باز کردن قفل آیفون یک داعشی دیگر ۵۱
ترکیه کشوری که بیشترین آلودگی به بات‌ها را دارد! ۵۲
دستگیری مظنون اصلی سرقت ابزارهای نفوذ سازمان NSA ۵۳
چانه‌زنی یک میلیارد دلاری شرکت Verizon برای خرید یاهو پس از رسوایی امنیتی ۵۴
از این پس وزرای بریتانیا نمی‌توانند ساعت اپل را هم در جلسات کابینه دولت همراه خود داشته باشند ۵۵
اجازه‌ی هک پیام‌رسان فیس‌بوک، اسکایپ و واتس‌اپ توسط قانون ضدتروریسم روسیه ۵۶
ترکیه برای سانسور کردن افشاگری گروه RedHack سرویس‌های گیت‌هاب، دراپ‌باکس و گوگل درایو را مسدود کرد. ۵۷
آمریکا رسماً دولت روسیه را در هک‌های مربوط به انتخابات مقصر می‌داند! ۵۸
پویش OilRig دولت آمریکا و شبکه‌های انرژی را هدف قرار داده است ۶۰

فصل چهارم: اخبار فنی

ادوبی ۸۱ آسیب‌پذیری آکروبات، فلش و ریدر را رفع کرد ۶۳
اصلاح آسیب‌پذیری دور زدن احراز هویت SAP پس از ۳ سال! ۶۵
محققان از ماژول RKP برای نفوذ به Samsung KNOX استفاده کردند ۶۶
وصله آسیب‌پذیری منع سرویس در اندروید از سوی گوگل ۶۸
وصله‌های روز سه‌شنبه: مایکروسافت 5 آسیب‌پذیری روز-صفرم را وصله کرد ۷۰
هشدار سیسکو در خصوص آسیب‌پذیری‌های جدی در سوئیچ‌های Nexus ۷۲

فصل پنجم: اخبار تحلیلی

آلودگی بیش از ۱۰۰ فروشگاه برخط به بدافزار جدید Magecart ۷۵
کمپین هرزنامه‌ی آلوده به بدافزار Eko کاربران فرانسوی را هدف حمله قرار داده است ۷۷
مرد میانی واقعی: انتقال جزئیات ورود از طریق بدن انسان ۷۸
به لطف موتور جستجوی Shodan بستر خدمات باج‌افزاری Encryptor غیرفعال شد ۸۰

فهرست مطالب

آسیب‌پذیری بیش از ۵۰۰ هزار دستگاه اینترنت اشیاء به بات‌نت Mirai.. ۸۲
فراتر از تشخیص مبتنی بر امضاء ۸۴
وب‌گاه‌های هک‌شده‌ی وردپرس، کاربران را به سمت فروش .. ۸۵
کلید ویندوز هدایت می‌کنند!
بدافزار جاوا اسکریپت رایانه‌ی شما را خاموش خواهد کرد، ۸۶
اگر به فرآیند مربوط به آن خاتمه دهید
باج‌افزار WildFire تحت عنوان باج‌افزار جدید Hades Locker ۸۸
احیاء شده است!
سوءاستفاده‌ی بدافزارها از بستر عیب‌یابی ویندوز برای ۹۰
آلوده کردن کاربران
مبهم‌سازی: بهترین دوست بدافزارها (بخش 1). ۹۲
باج‌افزار DXXD حتی پرونده‌های شبکه‌های اشتراکی نگاشت‌نشده ۹۴
را نیز رمزنگاری می‌کند
کارگزارهای کنار گذاشته شده‌ی C&C موبایل، فرصتی حی و ۹۶
حاضر برای مهاجمان
استفاده از پرس‌وجوهای WMI توسط بدافزارها برای فرار از تشخیص. ۹۸
تبانیِ برنامه‌های موبایل، سازوکارهای معمول امنیتی را دور می‌زند! ۱۰۰
شکستنِ تکنولوژی JEA مایکروسافت برای نفوذ به سامانه‌ها. ۱۰۲
سوءاستفاده‌ی بدافزار FastPOS از Mailslots ویندوز برای سرقت داده‌ها. ۱۰۴

فصل اول

اخبار عمومی

اخبار عمومی

Pirate Bay، در فهرست وب‌گاه‌های مخرب تورنت

گوگل به کاربران هشدار داده است که از وب‌گاه توزیع محتوای بدنام و غیرمجاز The Pirate Bay دوری کنند، زیرا بر این باور است که این پایگاه مبتنی بر تورنت برای سلامت رایانه‌های شخصی مضر است.

Mountain View معمولاً این وب‌گاه تورنت را به عنوان نهاد مخربی معرفی نمی‌کند، اما در تعداد انگشت‌شماری که این وب‌گاه با انتشار تبلیغات گاهاً خطرناک خود به بدافزاری سرویس‌دهی کرده به شدت نسبت به آن هشدار داده است.

گوگل هشدار داد: «ممکن است نفوذگران سعی کنند تا شما را برای بارگیری نرم‌افزاری فریب دهند و یا اطلاعات شما نظیر گذرواژه‌ها، پیام‌ها، یا اطلاعات محرمانه‌ی کارت اعتباری‌تان را به سرقت ببرند.»

ممکن است بازدیدکنندگان از این وب‌گاه در بستر کروم با صفحه‌ی قرمزرنگ مرگ بدافزار مواجه شوند، صفحه‌ای که از کاربران می‌خواهد که هشدار به نمایش درآمده را برای رسیدن به The Pirate Bay کنار بزنند.

The Pirate Bay از مجموعه‌ی متنوعی از تبلیغات معمولی میزبانی می‌کند. همچنین پیوندهای بسیار به وب‌گاه‌های کلاه‌برداری مرتبط با سرمایه‌گذاری و آلودگی‌های جعلی در دستگاه‌های کاربران در این وب‌گاه به چشم می‌خورد.

در نهایت گوگل ماه گذشته به کمک سرویس Safe Browsing خود این وب‌گاه را از نوع مخرب معرفی کرد.

این غول دنیای فن‌آوری کماکان روی رقیب قدرتمند Pirate Bay، یعنی Extra Torrent هیچ برچسبی نگذاشته است، وب‌گاهی که تبلیغات مربوط به شبکه‌های خصوصی مجازی و نیز دوست‌یابی را رواج می‌دهد.

اخبار عمومی

انتشار لیبره‌آفیس ۵٫۳ در فوریه‌ی ۲۰۱۷

نسخه‌ی جدید بسته‌ی محبوب LibreOffice، یعنی 5.3، به زودی توسعه پیدا کرده و نخستین جلسه‌ی رفع اشکال آن ظرف دو هفته‌ی آینده برگزار خواهد شد.

صحبت از LibreOffice 5.3 است، که نسخه‌ی آزمایشی آلفای آن در ۱۷ اکتبر منتشر خواهد شد، این اتفاق چند روز قبل از اولین جلسه‌ی رفع اشکال این بسته رخ خواهد داد؛ ظاهراً این جلسه در روز جمعه، ۲۱ اکتبر برگزار خواهد شد. در طول جلسه‌ی رفع اشکال توسعه‌دهندگان و نفوذگران کلاه‌سفید آزمایش‌هایی را روی LibreOffice ترتیب می‌دهند و سعی می‌کنند بیشترین تعداد خطای ممکن را در این بسته‌ی پرکاربرد برطرف سازند.

در طول جلسات اختصاص داده شده، محققان همه‌ی سعی خود را می‌کنند تا اشکال‌های موجود را یافته و راجع به آن‌ها اطلاع‌رسانی کنند، تا به این ترتیب آن‌ها را به یک طریق جامع‌تر تأیید و گزارش نمایند. البته، هرچه‌قدر که یک گزارش اشکال پیچیده‌تر باشد، توسعه‌دهندگان راحت‌تر می‌توانند در زمان باقی‌مانده به انتشار نسخه‌ی اصلی اشکال‌های موجود را رفع نمایند.

جدول زمانی انتشار LibreOffice 5.3

چرخه‌ی توسعه‌ی LibreOffice 5.3 شامل یک نسخه‌ی آلفا است، هرگاه اولین جلسه‌ی رفع اشکال آن در اکتبر برگزار شود، دومین نسخه که یک انتشار بتا از این بسته است، که برای آزمایش عموم کاربران در ۲۱ نوامبر منتشر خواهد شد .

اگر بعد از انتشار نسخه‌ی ۱ بتا تعداد بی‌شماری آسیب‌پذیری در LibreOffice 5.3 کشف شود، احتمالاً یک نسخه‌ی ۲ بتا از این بسته را نیز در هفته بعد از آن، یعنی حول و حوش ۷ دسامبر خواهیم داشت.

بعد از آن، چرخه‌ی توسعه‌ی لیبره‌آفیس 5.3 با سه نسخه‌ی کاندید انتشار ادامه پیدا خواهد کرد، نخستین مورد برای کریسمس ۲۰۱۶ تدارک دیده شده است. در ژانویه‌ی ۲۰۱۷، ممکن است یک نشست رفع اشکال ترتیب داده شود و نیز دو نسخه‌ی کاندید انتشار دیگر در راه باشد. نسخه‌ی کاندید انتشار ۲ از LibreOffice 5.3 بایست در ۹ ژانویه از راه برسد، و سومین مورد از این گونه از نسخه‌های LibreOffice 5.3 در ۲۳ ژانویه‌ی ۲۰۱۷ به کاربران مشتاق ارائه خواهد شد.

چرخه‌ی توسعه‌ی LibreOffice 5.3 در انتهای ژانویه‌ی سال میلادی آینده به اتمام خواهد رسید، درست زمانی که انتشار نهایی از این بسته در ۱ فوریه ارائه شود. این نسخه‌ها به همراه کد منبعشان مانند همیشه برای توزیع‌های GNU/Linux و نیز macOS، و سامانه‌های عامل ویندوز مایکروسافت در دسترس خواهند بود.

خبرهای جدید راجع به لیبره‌آفیس را از همین وب‌گاه به اطلاع شما خواهیم رساند.

اخبار عمومی

مسنجر فیس‌بوک از روش رمزگذاری واتس‌اپ استفاده می‌کند

سال گذشته، شرکت تابعه‌ی فیس‌بوک یعنی واتس‌اپ اعلام کرد که یک قابلیت رمزگذاری انتها به انتها را راه‌اندازی کرده که باعث شده که واتس‌اپ به بزرگ‌ترین شبکه از نوع خود تبدیل شود.

قابلیت رمزگذاری به‌طور دستی برای هر مکالمه‌ای فعال می‌شود ولی این ویژگی به‌طور پیش‌فرض فعال نیست. مسنجر فیس‌بوک کاملاً بی سر و صدا این ویژگی انتخابی را به جدیدترین به‌روزرسانی خود اضافه کرده است؛ این به‌روزرسانی در ۲۸ سپتامبر ارائه شده است.

اگرچه آخرین به‌روزرسانی برای iOS و اندروید به صراحت از قابلیت‌های تازه صحبتی به میان نیاورده است، اما کاربرانی که برنامه‌های خود را به‌روز کرده‌اند می‌توانند از این ویژگی «سری» را در سمت راست و بالای صفحه‌ی «پیام‌های جدید» برای ارسال پیام‌های رمزشده‌ای استفاده کنند که نه فیس‌بوک و نه هر مجری قانونی نمی‌تواند از آن‌ها سر دربیارود.

وقتی کاربر برای اولین بار این ویژگی را فعال می‌سازد با چنین پیامی مواجه می‌شود: « پیام‌های شما در حال حاضر امن هستند، پیام‌های سری (Secret Conversations) از یک از دستگاه به دستگاه دیگر رمز می‌شوند.»

به‌روزرسانی تازه همچنین شامل یک زمان انقضا برای پیام‌ها است که این زمان بین ۵ ثانیه الی یک روز متغیر است.

اخبار عمومی

درخواست از کاربران اوبونتو و Systemd برای به‌روزرسانی لینوکس

کاربران اوبونتو باید از به‌روزرسانی جدید هسته‌ی لینوکس که روی سامانه‌های عامل تحت پشتیبانی آن اثرگذار است، آگاه باشند.

در اخبار همین وب‌گاه خواندید که یک آسیب‌پذیری تازه در systemd پیدا شده که می‌تواند یک سامانه را به کمک یک دستور خیلی کوتاه خاموش کند؛ دستوری که آن‌قدر کوتاه است که می‌توان آن را توییت کرد؛ کاربران اوبونتو بایست وصله‌های جدیدی را که برای هسته‌ی لینوکس ارائه شده نصب کنند تا سامانه‌های عامل آن‌ها به روال عادی بازگردد.

مدیر SSLMate و بنیان‌گذار لینوکس، اندرو آیر، موفق به کشف خطایی شده که توانایی لازم برای غیرفعال‌کردن تعدادی از دستورات مهم را داراست.

از آن‌جایی که برای سوءاستفاده از این شکاف باید دسترسی محلی داشت و این سوءاستفاده فقط باعث بی‌ثباتی سامانه می‌شود و به از دست رفتن داده‌ها نمی‌انجامد، آیر این شکاف را در رده‌ی شکاف‌هایی با شدت پایین قرار داده است.

با این وجود شکاف مورد بحث یک آسیب‌پذیری مهم است، زیرا کمبودهای جدی در معماری و توسعه‌ی systemd را پررنگ می‌کند. یک آسیب‌پذیری این‌چنینی نباید در مؤلفه‌های یک سامانه‌ی عامل مهم وجود داشته باشد، و اگر systemd از یک طراحی خوب برخوردار بود هرگز چنین امکانی وجود نداشت.

آیر گفت که این مسئله موجب نگرانی است، به خصوص وقتی که این سامانه مؤلفه‌های بی‌شماری از سامانه‌ی عامل لینوکس را جابه‌جا می‌کند.

به عبارت کوتاه‌تر، آیر به مدیران شبکه توصیه می‌کند تا مطمئن شوند که ویژگی به‌روزرسانی خودکار امنیتی را فعال کرده‌اند، به‌طوری که اصلاحیه‌های آسیب‌پذیری‌ها را دریافت می‌کنند.

آیر توصیه کرد که کاربران به قابلیت‌های قدیمی و غیراستاندارد systemd اعتماد نکنند، و به فکر جای‌گزینی systemd با یک جای‌گزین قوی‌تر در سال‌های آینده باشند.

بنا به گزارش‌های رسیده وصله‌ی مورد نظر در گیت‌هاب منتشر شده است.

کانونیکال هم امروز یک سری از وصله‌های ویژه‌ی آسیب‌پذیری‌های هسته‌ی لینوکس را معرفی کرد که روی سامانه‌های عامل تحت پشتیبان اوبونتو اثرگذارند.

این آسیب‌پذیری‌ها شامل یک بازگشت بی‌نهایت در VLAN هسته‌ی لینوکس و نیز پیاده‌سازی پردازش GRO از TEB، یک وضعیت استفاده بعد از آزادسازی در کد کنترل صف ارسال مجدد TCP هسته‌ی لینوکس، یک شرایط رقابتی در درایور کنسول یا همان پیش‌ران s390 SCLP از هسته‌ی لینوکس، و یک شرایط رقابتی در زیرسامانه‌ی بازبینی هسته‌ی لینوکس می‌باشد.

اگـر ایـن آسـیب‌پذیری‌ها اصلاح‌نشـده باقـی بماننـد، ایـن شـکاف‌ها می‌تواننـد بـه نفوذگـر دارای دسترسـی از راه دور اجـازه دهنـد تـا سـامانه را بـا توقـف عمل‌کـرد مواجـه سـازد، و یـا اطلاعـات حسـاس را بازیابـی نمایـد.

بـه کاربـران توصیـه می‌شـود تـا سـامانه‌های خـود را در اسرع وقـت بـه‌روز نماینـد.

اخبار عمومی

غیرفعال شدن ویژگی ارسال مجدد رایانامه‌ی یاهو کار را برای ترک این سرویس سخت‌تر می‌کند

یاهو سامانه‌ی ارسال مجدد خودکار رایانامه را غیرفعال کرد؛ این قابلیت به کاربران یاهو اجازه می‌دهد تا یک نسخه‌ی رونوشت از رایانامه‌های ورودی را از یک حساب کاربری به حساب‌های دیگر ارسال مجدد نمایند.

این شرکت صاحب‌نام در چند هفته‌ی گذشته با انتشار اخبار ناخوشایند راجع به سرویس رایانامه‌اش مواجه شده است. ماه گذشته این شرکت یک نقض عظیم داده در سال ۲۰۱۴ را تأیید کرد که باعث شده بود جزئیات حساب کاربری بیش از ۵۰۰ میلیون کاربر یاهو به بیرون درز کند. اگر کاربران با شنیدن این خبر به ترک این سرویس مجاب نشده باشند با خبر تکان‌دهنده‌ی هفته‌ی گذشته حتماً بایست در تصمیم خود تجدید نظر کرده باشند؛ این شرکت مطرح به درخواست یک سرویس اطلاعاتی آمریکا رایانامه‌های صدها میلیون نفر از کاربران خود را پویش کرده است.

این خبرها کافی است تا کاربران وفادار رایانامه‌ی یاهو به دنبال جای‌گزینی مانند جی‌میل یا مایکروسافت اوت‌لوک باشند.

رایانامه‌ی یاهو ارسال مجدد خودکار را غیرفعال می‌سازد؛ به این ترتیب ترک یاهو دشوار می‌شود.

در حالی که کاربران رایانامه‌ی یاهو در تلاش برای ترک این سرویس هستند، این شرکت شرایط را برای مهاجرت به یک سرویس رایانامه‌ی دیگر دشوارتر نموده است.

دلیل این دشواری این است که از ابتدای اکتبر، یاهو قابلیت ارسال مجدد رایانامه را غیرفعال ساخته است؛ این قابلیت به کاربران اجازه می‌دهد تا به‌طور خودکار رایانامه‌های دریافتی حساب کاربری یاهوی خود را به حساب‌های دیگرشان هدایت نمایند.

به عبارت دیگر، فقط کاربرانی که این قابلیت را در گذشته فعال کرده بودند با این دردسر مواجه نیستند، اما کاربرانی که هم‌اکنون می‌خواهند ارسال مجدد رایانامه را فعال کنند دیگر چنین اختیاری ندارند.

یاهو در تلاش برای انجام معامله با ورایزون

حرکت یاهو در راستای از کار انداختن ویژگی ارسال مجدد خودکار رایانامه می‌تواند تلاشی برای فعال نگه داشتن حساب‌های کاربری یاهو باشد؛ زیرا هرگونه آسیبی به این شرکت در این برهه‌ی زمانی می‌تواند عواقب ناخوشایندی داشته باشد، زیرا این روزها یاهو به شدت در تلاش برای فروش خود به ورایزون است.

قرارداد یاهو هنوز منعقد نشده است، و همان‌طور که در خبرهای پیشین این وب‌گاه گفتیم ورایزون در صدد گرفتن یک تخفیف ۱ میلیاردی از یاهو است.

به عنوان یک راه حل پیشنهادی به شما می‌گوییم که پاسخ‌گوی تعطیلات سرویس خود را، به جای پاسخ‌گویی خودکار به رایانامه‌ها به وسیله‌ی یک یادداشت درباره‌ی

آدرس رایانامه‌ی جدیدتان، فعال سازید.

حساب یاهوی خود را قبل از این‌که خیلی دیر شود پاک کنید

شما می‌توانید این فرآیند ارسال مجدد را فراموش کنید و به آسانی هرچه تمام‌تر حساب رایانامه‌ی یاهوی خود به کلی حذف نمایید؛ شاید یاهو این ویژگی را نیز به زودی از کار بیاندازد.

به گزارش رسانه‌ها، کاربران مخابرات بریتانیا، که یاهو را به عنوان سرویس رایانامه‌ی خود انتخاب کرده بودند، قادر نیستند ارسال مجدد خودکار رایانامه را فعال سازند و یا حتی به گزینه‌ای مبنی بر پاک‌سازی حساب‌های کاربری دسترسی ندارند.

پس پیشنهاد ما به شما این است که تا فرصت باقی است به فکر باشید.

اخبار عمومی

سرویس پانورامیوی گوگل تعطیل خواهد شد

گوگل قصد دارد وب‌گاه به اشتراک گذاری عکس پانورامیو را حذف کند، این تصمیم موجی از خشم و اندوه را میان کاربران مشتاق به این سرویس به وجود آورده است.

این هفته طرف‌داران پانورامیو با این اطلاعیه مواجه شدند: «پانورامیو در حال بسته‌شدن است»، تا تاریخ ۴ نوامبر این مهلت به پایان می‌رسد. این جمله از طریق پستی در انجمن گفت‌وگوی به گوش کاربران رسید و آن‌ها را ناراحت و عصبانی کرد.

ممکن است شما هیچ‌وقت اسم پانورامیو را نشنیده باشید، اما احتمالاً به شما سود رسانیده است. تصاویر این وب‌گاه دارای یک منبع اولیه در Google Maps است. پانورامیو به این دلیل سودمند بود که اجازه می‌داد تصاویر دارای برچسب‌های موقعیت مکانی باشند و شما بتوانید عکس‌های متعلق به یک نقطه‌ی خاص را ببینید. پانورامیو در سال ۲۰۰۷، و پیکاسا در سال ۲۰۰۴ راه‌اندازی شدند، و اوایل کار خود سرویس محبوب گوگل برای به اشتراک‌گذاری عکس بودند، اما گوگل هر دو را به تدریج و به نفع Google Photos کنار گذاشت.

انجمن کاربران به طرز چشم‌گیری سرویس‌های برخط را از طریق افزودن محتوای ارزش‌مند بدون هیچ هزینه‌ای برای گوگل، بهبود بخشیده‌اند. این انجمن به جذب اعضای جدید و ایجاد روابط اجتماعی نیاز دارد تا کماکان همچنان سرویس مربوطه را در رأس قدرت نگه دارد. اما این امتیازها هنگام بسته‌شدن آن انجمن به یک مشکل مضاعف تبدیل می‌شوند، حتی انجمن‌هایی که تنها بخش کوچکی از کاربران یک سرویس را شامل می‌شوند. مرگ پانورامیو جای هیچ تعجبی را باقی نمی‌گذارد؛ در ۲۰۱۴، گوگل سعی داشت تا پانورامیو را منسوخ کند. گوگل که با این تصمیم خود موجب اعتراض بیش از ۱۰هزار کاربر خود شد، حاضر شد کنار گذاشتن این وب‌گاه را به سال ۲۰۱۵ موکول کند، اما به وضوح مشخص بود که وب‌گاه پانارامیو دیگر یکی از الویت‌های گوگل نیست.

برخی از کاربران با وجود اطلاع از این ماجرا به این سرویس وفادار ماندند. بعضی از این کاربران به خاطر این اقدام از گوگل کینه به دل گرفته‌اند.

یکی از کاربران در این رابطه گفت: «من میلیون‌ها بازدید داشتم، برخی از عکس‌های من بیش از ۱۰۰هزار بار دیده شده بودند و دارای سطح ۵ بودند، من تعداد بی‌شماری خطا در Maps را به گوگل گوش‌زد کرده بودم و حالا گوگل به من می‌گوید خداحافظ! ما دیگر به تو نیازی نداریم، چون در حال حاضر فقط تصویر رستوران‌ها را می‌پذیریم.»

«من خوشحالم که دو سال پیش بیشتر تصاویرم را پاک کردم، و حالا فقط بایست ۲۰ عکس باقی‌مانده را حذف کنم.»

گوگل در این‌باره هیچ اظهار نظری نکرده است.

انجمن‌های به اشتراک‌گذاری تصویر بسیاری برای افرادی

وجـود دارد کـه علاقـه‌ای بـه Google Photos ندارنـد، از جملـه‌ی ایـن انجمن‌هـا می‌تـوان بـه فلیکـر یاهـو، اینسـتاگرام فیس‌بـوک و 500px اشـاره کـرد.

یکـی از وب‌گاه‌هایـی کـه بـه پنـاه‌گاه کاربـران پانورامیـو مبـدل شـده، وب‌گاه فرانسـوی بـه اشـتراک‌گذاری تصویـر Ipernity اسـت. بـه نظـر می‌رسـد ایـن سرویـس دارای ویژگی‌هایـی اسـت کـه کاربـران پانورامیـو آن‌هـا را می‌پسـندند.

اخبار عمومی

آیا در جست‌وجوی بهترین ابزارهای رمزنگاری هستید؟

در طول چند سال گذشته، کاربران اینترنت در هر نقطه از جهان به‌طور فزاینده‌ای از اهمیت حریم خصوصی و امنیت آگاه شده‌اند، شاید دلیل این آگاهی نظارت گسترده و نظارت از سوی سازمان‌های دولتی بزرگ باشد، که باعث شده کاربران بیش از پیش سرویس‌ها و نرم‌افزارهای رمزنگاری را ضمیمه‌ی کار خود نمایند.

در این میان نفوذگران هم بی‌کار ننشسته‌اند و از این موقعیت با ایجاد و توزیع نسخه‌های جعلی از ابزارهای رمزگذاری سوءاستفاده کرده‌اند تا با این شیوه بتوانند بیشترین قربانی ممکن را داشته باشند.

آزمایشگاه کسپرسکی یک گروه تهدید پیشرفته‌ی مستمر (APT) را کشف کرده است؛ این گروه برای هدف قرار دادن کاربرانی که از نرم‌افزارهای طراحی‌شده برای رمزگذاری داده و ارتباطات استفاده می‌کنند، نهایت تلاش خود را به خرج داده است.

سال‌های سال است که یک گروه تهدید پیشرفته‌ی مستمر با نام StrongPity از حملات مبتنی بر گودال آبیاری یا همان watering-hole، نصب‌کننده‌های آلوده، و بدافزار استفاده کرده است تا کاربران نرم‌افزارهای رمزگذاری را با نفوذ به وب‌گاه‌های مجاز یا راه‌اندازی وب‌گاه‌های مقلد و مخرب خودشان هدف حمله قرار دهند.

حملات watering-hole برای فریب دادن گروه خاصی از کاربران به بازدید از وب‌گاه‌های مورد علاقه‌ی نفوذگران و یا هدایت آن‌ها برای بارگیری‌های تحت نظارت نفوذگران طراحی شده است.

گروه تهدید پیشرفته‌ی مستمر StrongPity موفق شده کاربران اروپا، شمال آفریقا، و خاورمیانه را هدف حمله قرار دهد، همچنین به دو نرم‌افزار رمزنگاری رایگان WinRAR و TrueCrypt در حملات متمایز حمله کند.

مدت مدیدی است که WinRAR و TrueCrypt میان کاربران آگاه به حریم خصوصی و امنیت محبوبیت دارند. WinRAR بیشتر به خاطر قابلیت‌های آرشیوسازی (بایگانی) که منجر به رمزگذاری پرونده‌ها با رمزهای AES ۲۵۶ بیتی می‌شود شهرت دارد؛ این در حالی است که TrueCrypt یک ابزار رمزگذاری تمام‌دیسک است که همه‌ی پرونده‌های روی یک هارد دیسک یا دیسک سخت را قفل می‌نماید.

StrongPity با راه‌اندازی وب‌گاه‌های جعلی که بسیار دقیق عمل‌کرد وب‌گاه‌های بارگیری مجاز را تقلید می‌کنند، توانسته کاربران به بارگیری نسخه‌های مخرب این برنامه‌های رمزنگاری فریب دهد تا کاربران داده‌هایشان را به کمک یک نسخه‌ی آلوده به تروجان از برنامه‌های WinRAR یا TrueCrypt رمزگذاری نمایند، و به این ترتیب به نفوذگران اجازه دهند تا داده‌های رمزشده را پیش از وقوع رمزنگاری مورد جاسوسی قرار دهند.

این گروه PAT پیش از این هم در اواخر سال ۲۰۱۵ میلادی حملات گودال آبیاری در پوشش TrueCrypt را راه‌اندازی

کرده بود، اما فعالیت‌های مخرب این گروه در اواخر تابستان ۲۰۱۶ به اوج خود رسید.

بین جولای و سپتامبر، ده‌ها تن از بازدیدکنندگان از tamindir[.]com به true-crypt[.]com تغییر مسیر داده شده‌اند، جای تعجب وجود ندارد که تقریباً همه‌ی تمرکز روی سامانه‌های رایانه‌ای موجود ترکیه بوده است و تنها بخش اندکی از این قربانی‌ها متعلق به هلند بوده‌اند.

با این حال، این گروه نفوذگر در مورد نرم‌افزار WinRAR به جای هدایت کاربران به وب‌گاه‌های تحت کنترل خود، اختیار وب‌گاه مجاز winrar.it را در دست گرفته تا یک نسخه‌ی مخرب از پرونده‌ی خودشان را میزبانی نمایند.

وب‌گاه winrar.it بیشتر کاربران مستقر در ایتالیا، و تعدادی از کاربران کشورهایی نظیر بلژیک، الجزایر، تونس، فرانسه، مراکش، و ساحل عاج را آلوده کرده است؛ اما نفوذگران پشت پرده‌ی winrar.be کاربران بلژیکی، الجزایری، مراکشی، هلندی، و کانادایی را آلوده کرده‌اند.

با توجه به گزارش کسپرسکی، امسال بیش از ۱۰۰۰ سامانه به بدافزار StrongPity آلوده شده‌اند. پنج کشور نخستی که توسط این گروه آسیب دیده‌اند عبارتند از ایتالیا، ترکیه، بلژیک، الجزایر، و فرانسه.

گروه تهدید پیشرفته‌ی مستمر StrongPity بدافزار خود را با گواهی‌نامه‌های دیجیتال غیرمعمولی امضا کرده‌اند، اما این گروه از این گواهی جعلی استفاده‌ی مجدد نکرده است. این بدافزار مؤلفه‌هایی همچون یک در پشتی، کی‌لاگر، سارق داده، و سایر برنامه‌های نرم‌افزاری مربوط به رمزنگاری مانند سرویس‌گیرنده‌ی putty SSH، سرویس‌گیرنده‌ی FTP فایل‌زیلا، برنامه‌ی انتقال پرونده‌ی امن Winscp و سرویس‌گیرنده‌های راه دور را بارگیری می‌کند.

این بدافزار نه‌تنها کنترل سامانه را در اختیار نفوذگران قرار می‌دهد، بلکه به آن‌ها اجازه می‌دهد تا محتوای دیسک را بربایند و بدافزارهای دیگری را بارگیری کنند که منجر به ربودن ارتباطات و اطلاعات تماس می‌شوند.

بنابراین، به کاربرانی که از وب‌گاه‌ها بازدید می‌کنند و نرم‌افزارهای رمزگذاری رایگان را بارگیری می‌کنند توصیه می‌شود تا هم اعتبار وب‌گاه‌های توزیع محتوا را بررسی کنند، و هم یکپارچگی پرونده‌های بارگیری شده را امتحان نمایند.

وب‌گاه‌های بارگیری که از PGP یا هر مجوز امضای کد دیجیتال قوی استفاده نمی‌کند، می‌بایست ضرورت انجام این کار را برای منافع خود و نیز کاربرانشان در الویت قرار دهند.

اخبار عمومی

آیا می‌خواهید از به‌روزرسانی خودکار به macOS Sierra نجات پیدا کنید؟

آیا به تازگی یک افت سرعت محسوس را در مک‌بوک خود حس کرده‌اید؟ شما در این حس تنها نیستید!
اپل «پیش-بارگیری» جدیدترین نسخه از سامانه‌ی عامل ویژه‌ی رومیزی خود، macOS 10.12 Sierra، را در پس‌زمینه آغاز کرده است؛ شاید تذکر این نکته برای کاربرانی که هنوز از نسخه‌ی ال کاپیتان بد نباشد.
اگر به‌روزرسانی خودکار را در مک خود فعال کرده‌اید، یک پرونده‌ی بزرگ ۵ گیگابایتی به‌طور مرموز و در پس‌زمینه در رایانه‌ی شما بارگیری می‌شود، جالب توجه است که از پهنای باند اینترنت شما برای بارگیری این پرونده‌ی ناخواسته استفاده می‌شود.
اپل این حرکت را این‌گونه توجیه کرد که بارگیری خودکار رسیدن به سامانه‌های عامل به‌روز را برای کاربران راحت‌تر از پیش خواهد کرد و آن‌ها را به به‌روزرسانی سامانه‌هایشان تشویق می‌کند.
خبر خوب این است که این به‌روزرسانی به‌صورت خودکار و بدون کسب اجازه از شما نصب نمی‌شود. هرگاه این نسخه به‌طور خودکار در پس‌زمینه بارگیری شود، کاربرانی که نسخه‌ی 10.11.5 یا نسخه‌های بعدی ال کاپیتان را اجرا می‌کنند، یک اطلاع‌رسانی را دریافت می‌کنند که بیان می‌کند macOS Sierra آماده‌ی نصب است.
تمام آن کاری که بایست انجام دهید این است که روی دکمه‌ی نصب کلیک کنید تا به‌روزرسانی شروع شود.
خوشبختانه این ویژگی به‌روزرسانی خودکار به اندازه‌ی کافی هوشمند است که بتواند روی رایانه‌های تحت مکی بارگیری شود که دارای فضای ذخیره‌سازی کافی بوده و مشخصات سخت‌افزاری لازم برای نصب macOS Sierra را در خود دارند.
بنابراین در صورتی که رایانه‌ی مک مورد نظر از فضای کافی برخوردار نباشد، نصب‌کننده‌ی Sierra پاک خواهد شد.
مایکروسافت نیز ساز و کار مشابهی را برای کاربران ویندوز ۷ و ۸ به کار گرفته است؛ در حقیقت مایکروسافت هم نصب ویندوز ۱۰ را از زمان راه‌اندازی این نسخه به کاربران تحمیل نمود و اعتراض گسترده‌ای را به وجود آورد.

چگونه از بارگیری خودکار MacOS Sierra جلوگیری کنیم؟

این فرآیند به‌روزرسانی خودکار کمی آزاردهنده به نظر می‌رسد، زیرا ممکن است کاربر به هیچ وجه قصد نداشته باشد که سامانه‌ی مک خود را به همین زودی به‌روز نماید.
اگر مهیای ارتقاء به جدیدترین نسخه از macOS نیستید، یا می‌خواهید این نسخه را بعداً بارگیری کنید، می‌توانید به راحتی نصاب Sierra را به‌صورت دستی پاک کنید تا به این ترتیب وادار به نصب آن نشوید.
برای پاک‌سازی نصب‌کننده‌ی Sierra به← Finder

Applications بروید، سپس به دنبال برنامه‌ای بگردید که «Install macOS Sierra» نام دارد، بعد این برنامه را به سطل زباله‌ی خود منتقل نمایید، و در پایان سطل زباله‌ی خود را خالی کنید تا هیچ اثری از Sierra باقی نماند.

اگر می‌خواهید که یک به‌روزرسانی حجیم ۵ گیگابایتی در رایانه‌تان بارگیری نشود و دیگر نیازی نباشد که شما فرآیند نصب را لغو کنید، می‌توانید بارگیری‌های خودکار را در اپ‌استور غیرفعال کنید تا از بارگیری‌های ناخواسته جلوگیری شود.

برای از کار انداختن این ویژگی، می‌توانید به مسیر System Preferences > App Store > Automatically check for updates رفته و تیک گزینه‌ی «بارگیری به‌روزرسانی‌های تازه در پس‌زمینه»را بردارید.

تمام شد، موفق شدید!

حالا دیگر رایانه‌ی شما به‌صورت خودکار macOS Sierra را بارگیری نمی‌کند و شما را وادار به نصب آن نمی‌کند. اما در آینده اگر نظرتان عوض شد می‌توانید به حالت به‌روزرسانی خودکار برگردید.

اخبار عمومی

اپل مرور خصوصی Safari در iOS 10 را تضعیف کرد!

براساس گفته‌ی تحلیلگران گروه IntaForensics، علاوه بر توقف سامانه‌ی گذرواژه برای پشتیبان‌گیری از iTunes، به نظر می‌رسد که اپل مرور خصوصی Safari در iOS 10 را نیز تضعیف و کمتر کرده است.

مشکل اصلی که اپل کشف کرده، مربوط به نحوه‌ی ذخیره‌سازی اطلاعات جلسات مرور خصوصی در Safari و به عبارت دیگر مربوط به حالت تعلیق URL ها است. این URL ها مربوط به زبانه‌هایی است که توسط کاربر بسته شده است اما مرورگر همچنان آن‌ها نگه داشته تا کاربر برگشته و از آن‌ها استفاده کند و در جلسه‌ی مرور خصوصی و یا عمومی خود پیش برود.

اینک Safari پیوندهای مربوط به جلسه‌های مرور خصوصی را در پایگاه داده خود ذخیره می‌کند!

محققان توضیح دادند که در نسخه‌های قبلی iOS، فهرست مربوط به جلسه‌های مرور خصوصی و URL های حالت تعلیق در پرونده‌ای با نام Plist نگهداری می‌شد. به محض اینکه کاربر زبانه‌ی جلسه‌ی مرور خصوصی را می‌بست، iOS این رکوردها را از پرونده‌ی Plist حذف می‌کرد.

این موارد در iOS 10 که اواخر ماه گذشته منتشر شد، تغییر کرد. محققان می‌گویند Safari به ذخیره‌ی اطلاعات جلسه‌های مرور خصوصی و URL های تعلیق در پایگاه داده خود می‌پردازد.

محققان IntaForensics گفتند که درحالی‌که اپل سعی و تلاش خود را برای حذف رکوردهای URL های حالت تعلیق از پایگاه داده می‌کند، به‌عنوان یک اقدام احتیاطی، این رکوردها را با داده‌های تصادفی رونویسی نمی‌کند.

ابزارهای جرم‌شناسی می‌توانند پیوندهای جلسه مرور خصوصی قبلی را بازیابی کنند!

این قابلیت به یک مهاجم اجازه می‌دهد با استفاده از ابزارهای جرم‌شناسی یا بازیابی پایگاه داده، رکوردهای حذف‌شده‌ی را نجات دهند. اگر Safari استفاده از Plist را ادامه می‌داد، این کار از لحاظ فنی غیرممکن بود.

محققان می‌گویند یک ابزار بازیابی پایگاه داده با نام XRY صفحات وب بسته‌شده را بازیابی کرد. بخش تاریخچه‌ی مرورگر Safari چه شما در حالت خصوصی و چه عمومی از صفحه‌ای دیدن کرده باشید، بدون استفاده از ابزارهای جرم‌شناسی به‌روز و قوی، قابل بازیابی است.

این کشف جدید، برگی دیگر از شکایت‌های انباشته‌شده در دفتر مرکزی اپل مربوط به iOS 10 است. علاوه بر عملکرد ضعیف، به‌نظر می‌رسد iOS 10 حفره‌های امنیتی و حریم خصوصی جدیدی در محبوب‌ترین محصول شرکت اپل ایجاد کرده است.

محققان امنیتی قبلاً کشف کردند که سامانه‌ی پشتیبان‌گیری iOS iTunes از یک سامانه‌ی گذرواژه‌ی

جایگزین استفاده می‌کند که 2500 بار برای کرک کردن راحت‌تر است. همچنین نقص دیگری که وجود دارد در قابلیت پیش‌نمایش پیوندها در پیام‌رسان iMessage است که برخی از اطلاعات کاربر را افشاء می‌کند.

اخبار عمومی

سرویس Spotify قربانیان را در دام حملات تبلیغاتی می‌اندازد!

افرادی که از سرویس موسیقی برخط Spotify استفاده می‌کنند، شاهد تبلیغات مخربی هستند که به‌طور خودکار یک مرورگر وب را باز کرده و آن‌ها را به وب‌گاهی مملو از بدافزار هدایت می‌کند.

Spotify که سرویس موسیقی برخط freemium نیز نامیده می‌شود و کاربران با استفاده از آن می‌توانند در دستگاه‌های مختلف همچون کامپیوترها، گوشی‌های تلفن همراه، تبلت‌ها و حتی تلویزیون‌ها به موسیقی گوش دهند. این کاربران می‌خواهند در ازای پرداختی که انجام می‌دهند از موسیقی لذت ببرد ولی پول پرداخت نکرده‌اند که تبلیغات مختلفی را مشاهده کرده و با آن‌ها تعامل داشته باشند.

در حالت عادی، کاربر برای مشاهده‌ی یک تبلیغ باید روی آن کلیک کند تا آن تبلیغ در یک مرورگر جدید باز شود، اما برخی کاربران رایگان Spotify اخیراً متوجه شده‌اند تبلیغاتی که آن‌ها مشاهده می‌کنند، متفاوت رفتار می‌کند. به‌ویژه اینکه این تبلیغات مرورگر جدیدی را اجرا می‌کنند که این اجرا بدون تعامل کاربر صورت می‌گیرد.

یک کاربر در انجمن Spotify گفته است: «این مسئله چند ساعت قبل شروع شد. اگر شما از Spotify رایگان استفاده می‌کنید، این برنامه مرورگر جدیدی حاوی بدافزار و ویروس‌های مختلف را باز خواهد کرد. برخی از این بدافزارها برای اجرا شدن و خطرساز بودن نیازی به فعالیت کاربر ندارد.»

سایر کاربران نیز چنین رفتار مشابهی را گزارش کرده‌اند و Spotify نیز تایید کرده که این رفتار برخی کاربران را تحت تاثیر قرار داده است. Spotify گفت: «این کاربران تجربه‌ی باز شدن یک وب‌گاه pop-up در مرورگر پیش‌فرض را شاهد هستند. ما مبدأ این مسئله را پیدا کردیم و درحال از کار انداختن آن هستیم. ما نظارت بر شرایط را ادامه می‌دهیم.»

این حادثه مثالی از یک پویش تبلیغاتی است که می‌تواند تنها از طریق یک وب‌گاه ضربه بزند. تا زمانی‌که برنامه‌های کاربردی به تبلیغات سرویس بدهند و مهاجمان این تبلیغات را در شبکه‌ها بقبولانند، تبلیغات وجود خواهد داشت. مهاجمان کد مخرب را داخل آگهی‌های ظاهراً قانونی مخفی می‌کنند و کاربران با دستگاه‌های آسیب‌پذیر قیمت آن را پرداخت می‌کنند.

این تبلیغات مخرب تنها کاربران را به سمت وب‌گاه‌هایی که قصد مشاهده‌ی آن را ندارند، هدایت نمی‌کند بلکه دستگاه کاربر را مجبور به بارگیری بدافزارهایی می‌کند که محققان آن را drive-by attacks می‌نامند. حتی نیازی نیست که کاربر قربانی با تبلیغات مخرب تعامل داشته باشد، چرا که اسکریپت مخفی داخل آن تمام کارها را به‌طور خودکار انجام خواهد داد.

اسکار آندویزا تحلیلگر بدافزار در Avira اشاره کرد که

سادگی این حادثه در رفتار غیرطبیعی در زمان نمایش تبلیغ است. اما در حال حاضر شاهد تبلیغات تهاجمی هستیم که هرزنامه یا کلاه‌برداری هستند و به‌طور خودکار و بدون رضایت کاربر در مرورگرها باز می‌شوند.»

آندویزا همچنین اشاره کرد که Spotify حق داشت که سریع‌تر به این مسئله رسیدگی کند و به‌طور مستقیم این تبلیغات مشکوک را کاهش دهد. برخی از این تبلیغات که در داخل برنامه و در نوار مشکی رنگ نمایش داده می‌شد، اینک بسته شده است.

در شرایطی که این تبلیغات وجود دارد، کاربران با به‌روز نگه داشتن برنامه‌ها و سامانه عامل خود می‌توانند از خود حفاظت کنند. همچنین کاربران برای حفاظت بیشتر می‌توانند یک راه‌حل ضدبدافزاری را نصب و نگهداری کنند.

اخبار عمومی

به دنبالِ «طوفان متیو»، رایانامه‌های مخرب این طوفان نیز در راه است!

همان‌طور که طوفان متیو، سواحل کارولینای جنوبی را درهم نوردید، مقامات از یک سری حملات سایبری علیه این ساکنین خبر دادند.

مجرمان سایبری هیچ بیمی ندارند و آماده‌ی هرگونه سوءاستفاده از یک رویداد تراژدیک به نفع خود هستند. کلاه‌برداران در گذشته رسانه‌های جالب را تحت عنوان حوادث تراژدیک مانند حمله ماراتن بوستون، مورد بهره‌برداری قرار دادند و یا در مورد سقوط پرواز MH17 هواپیمایی مالزی، مهاجمان از اخبار این رویداد به‌عنوان طعمه‌ای در حملات هرزنامه‌ای و فیشینگ استفاده کردند.

در این ساعات طوفان متیو بذر مرگ و نابودی را در مسیر خود پاشیده و رسانه‌ها به‌روزرسانی‌های مختلف از وضعیت این منطقه آسیب‌دیده را گزارش می‌دهند. مجرمان سایبری این شرایط را به خوبی می‌شناسند و در حال تلاش برای بهره‌برداری از این وضعیت هستند.

به محض اینکه طوفان متیو سواحل کارولینای جنوبی را درنوردید، سازمان‌های اجرای قانون در خصوص یک سری حملات سایبری علیه ساکنان هشدار دادند. مجرمان سایبری از طریق رایانامه‌ها، کاربران را در معرض خطر قرار می‌دهند و ادعا می‌کنند که به‌روزرسانی از شرایط و به‌ویژه رخداد سیل محلی را گزارش می‌کنند.

فرماندار نیکی هالی، یکشنبه در یک کنفرانس مطبوعاتی توضیح داد که فردی یک شبه پویش‌های مخرب را راه‌اندازی کرده است. در گزارش زنده اخبار، اظهارات هالی این‌گونه بیان شد: «افراد در حال دریافت رایانامه‌هایی هستند که در این رایانامه‌ها به‌روزرسانی در خصوص زمان قطع برق اعلام شده و گفته شده اگر می‌خواهید از این به‌روزرسانی مطلع شوید بر روی این پیوند کلیک کنید. اگر روی این پیوندها کلیک کنید مهاجمان خواهند توانست به کامپیوتر شما وارد شوند.»

البته، کلاه‌برداران در حال اجرای یک پویش فیشینگ نیز هستند که در آن پیام‌های مخرب می‌توانند شامل پیوند به وب‌گاه آلوده باشد. این وب‌گاه‌های آلوده ممکن است به بدافزارها و پرونده‌های مخرب سرویس بدهند که به محض باز شدن این صفحات، فرآیند آلوده شدن کامپیوتر قربانی شروع شود.

هرچند این مسئله یک هشدار محلی است ولی باید توجه داشت که این شیوه می‌تواند در شرایط این‌چنینی توسط مهاجمان در سرتاسر دنیا مورد استفاده قرار بگیرد. مراقب باشید! پرونده‌های ضمیمه را باز نکرده و بر روی پیوندهای موجود در رایانامه‌های ناخواسته کلیک نکنید. سامانه عامل و نرم‌افزارهای خود را به‌روزرسانی کرده و یک نرم‌افزار دفاعی نصب کنید.

اخبار عمومی

یک ابزار رایگان از کاربران مک در برابر نظارت وب‌کم حفاظت می‌کند!

ربودن وب‌کم یک کاربر، یکی از تکنیک‌ها برای نظارت بر کاربران است. در بسیاری از موارد مهاجم از چند نمونه بدافزار آگاه از وب‌کم استفاده می‌کند تا بی سر و صدا وب‌کم را روشن کرده و در ماشین قربانی شروع به ضبط صدا و ویدئو نماید.

با انجام این کار، همچنین یک چراغ LED که در کنار وب‌کم تعبیه شده روشن خواهد شد که نشانه‌ای برای فعال شدن وب‌کم است و کاربر متوجه می‌شود که یک عملیات غیرعادی و خارج از انتظار رخ داده است.

متخصص امنیت مک و مدیر بخش پژوهش Synack، پاتریک واردل قابلیت جدیدی را روز پنج‌شنبه در کنفرانس بین‌المللی بولتن ویروس 2016 ارائه کرد که می‌تواند در فرآیندهای macOS قانونی مورد سوءاستفاده قرار بگیرد. این قابلیت به مهاجم اجازه می‌دهد زمانی که برنامه‌هایی همچون Skype، FaceTime و یا Google Hangouts اجرا می‌شوند، بر روی وب‌کم قربانی سوار شود. با بدست آوردن وب‌کم علاوه بر اینکه مهاجم می‌تواند به جاسوسی بپردازد و به‌طور مثال مکالمه‌ی حساس و مهم بین شرکای تجاری را شنود کند، دیگر نگرانی در خصوص روشن شدن وب‌کم و چراغ LED ندارد.

در پاسخ به این تهدید، واردل دیروز یک ابزار نظارتی با نام OverSight را معرفی کرد که بر فرآیندهای داخلی macOS نظارت می‌کند تا وب‌کم و میکروفن ماشین را مدیریت کند و زمانی‌که فرآیندی به این سرویس‌ها دسترسی یافت، به کاربر هشدار دهد. در ادامه کاربر می‌تواند تصمیم بگیرد که به این جلسه اجازه دهد یا آن را مسدود نماید.

واردل گفت: «این ابزار می‌تواند فعال شدن وب‌کم و میکروفن را اعلام کند ولی چیزی که مهم‌تر است اینکه می‌تواند گزارش دهد کدام یک از فرآیندها به این سرویس دسترسی پیدا کرده و آیا این فرآیند توسط شخص دیگری ایجاد شده یا خیر. زمانی‌که این مسئله تشخیص داده شد، کاربر تصمیم می‌گیرد که این فرآیند را مسدود کند. همچنین گزارشی از این فعالیت در بخش syslog سامانه ثبت می‌شود تا مدیر محیط کاری در مراحل بعدی بتواند آن‌ها را تحلیل و بررسی نماید.»

واردل که در طول 2 سال گذشته دسته‌ای از ابزارهای امنیتی مک را منتشر کرده است، گفت ظهور نمونه‌های بدافزار مک مانند Crisis، Eleanor و Mokes همگی برای جاسوسی در بستر مک هستند و او را برآن داشته تا وقت زیادی را در این زمینه صرف کند.

Eleanor و Mokes نمونه‌های اخیر بدافزار مک هستند که این تابستان به ترتیب توسط شرکت‌های بیت‌دیفندر و کسپرسکی کشف شدند. Eleanor یک درب ِ پشتی تند و زشت است که یک سرویس مخفی Tor را ایجاد می‌کند و به مهاجم اجازه می‌دهد تا ماشین آلوده‌شده را از راه

دور کنترل نماید و همچنین نظارت‌های صوتی و ویدئویی نیز انجام می‌دهد. واردل گفت او همچنین ابزار متن‌باز Wacaw ارسال کرده که قابلیت ضبط تصویر و ویدئوها را فراهم می‌کند. در عین حال Mokes نیز یک درب ِ پشتی است که به سرقت داده‌ها، تصاویر، ویدئوها و صوت‌ها از ماشین‌های اپل، ویندوز و لینوکس آلوده‌شده می‌پردازد.

واردل می‌گوید: «ما اخیراً تمایل زیادی را در بدافزارهای مک مشاهده کرده‌ایم که به ضبط کارهایی که کاربر انجام می‌دهد، علاقه‌مند هستند.»

واردل گفت که کلید اصلی در این مسئله فعال کردن قانونی LED است که در شرایط ویژه‌ای توسط مهاجم و با دسترسی فیزیکی می‌تواند غیرفعال شود که مهاجم می‌تواند سامانه عامل و فرآیندهای سامانه را برنامه‌نویسی مجدد نماید. واردل گفت اپل مراحلی را برای کاهش این ریسک از طریق ایزوله کردن فرآیندها و سخت کردن هک آن‌ها انجام داده است.

کلید اصلی برای بدافزار جدید این است که مهاجم بداند به‌طور مثال چه موقع جلسه‌ی مربوط به استفاده از وب‌کم را آغاز کرده است. بدافزاری که توسط واردل در جولای سال 2015 از گروه هک leak بررسی شده است نشان داد که کد مخرب دوربین مشاهده شده است و فرآیندهای مرتبط با دوربین از طریق چارچوب بنیادی AV از اپل شمارش شده است. با استفاده از این چارچوب، مهاجم می‌تواند این فرآیندها را شمارش کرده و از طریق Apple CoreMediaIO Device Abstraction Layer از اعلان‌ها مطلع شود تا بداند یک جلسه کی شروع و کی تمام شده است تا بداند کی ضبط برای جاسوسی را شروع و تمام کند.

واردل می‌گوید: «این فرآیندها جالب‌ترین چیزی است که بدافزار باید آن را ضبط کند. او منتظر می‌ماند تا کاربر یک جلسه‌ی قانونی را شروع کند که از وب‌کم استفاده می‌نماید. زمانی که بدافزار این مسئله را تشخیص داد، شروع به ضبط و خروج داده می‌کند. این موضوع دیگر نیاز به دسترسی ریشه ندارد و نگرانی در خصوص روشن بودن چراغ LED نیز وجود ندارد و همچنین نشانه‌ای از اینکه بدافزار بر روی ترافیک سوار و در حال ضبط داده است نیز وجود نخواهد داشت.»

واردل می‌گوید ابزار Oversight می‌تواند فرآیند اولیه و متعاقبی را تشخیص دهد. هشداری که به کاربر نمایش داده می‌شود شامل نام فرآیندهایی است که از وب‌کم استفاده می‌کنند به‌طور مثال OSX/Mokes. همچنین این ابزار گزینه‌ی مسدود کردن فرآیند را نیز ارائه می‌کند.

فصل دوم

مدیریت امنیت

مدیریت امنیت

بی‌اعتمادی شهروندان انگلیسی به مسئولان دولتی در زمینه‌ی حفاظت از اطلاعات

براساس یک نظرسنجی گسترده که از سوی دفتر بازبینی ملی انگلستان منعکس شده، شهروندان بریتانیایی در توانایی دولت این کشور در کنترل داده‌های خصوصی‌شان اندکی شک دارند.

از میان ۱۵۰۰ شهروندی که در این نظرسنجی شرکت کردند فقط ۲۲٪ بر این باورند که دولت بریتانیا از ابزارهای مناسب برای توقف حملات سایبری برخوردار است.

فقط ۳۷٪ گفته‌اند که مطمئن هستند دولت این کشور اطلاعات شخصی آن‌ها را امن نگه می‌دارد؛ این در حالی است که ۳۲٪ معتقد هستند که این کشور قادر به به اشتراک گذاری ایمن اطلاعات بین نهادهای بخش عمومی نمی‌باشد.

این یافته‌ها به این خاطر به دست آمده که دولت این کشور در صدد آن است تا بر سهولت دسترسی بخش عمومی به اطلاعات شهروندان از طریق Digital Economy Bill بیافزاید.

با این حال، ۵۱٪ گفته‌اند که اگر بخش‌ها بتوانند اطلاعات بیشتری را به اشتراک بگذارند، استفاده از سرویس‌های عمومی دولت راحت‌تر خواهد بود.

اما یک گزارش جدید از دفتر بازبینی ملی انگلستان حاکی از آن است که شیوه‌های امنیت اطلاعات به کار گرفته شده توسط این کشور ضعیف هستند.

این دفتر کاشف به عمل آورده که دفتر کابینه‌ی این کشور در هماهنگ کردن تلاش‌های صورت‌گرفته از سوی بخش‌های مختلف دولت بریتانیا برای حفاظت از اطلاعات با شکست مواجه شده است؛ به نحوی که در سال‌های ۲۰۱۴ و ۲۰۱۵ در ۱۷ بخش دولتی بزرگ این کشور ۹۰۰۰ نقض داده رخ داده است.

حدود ۵۴٪ از نظردهندگان از امنیت به عنوان الویت نخست سرویس‌های برخط دولتی یاد کرده‌اند.

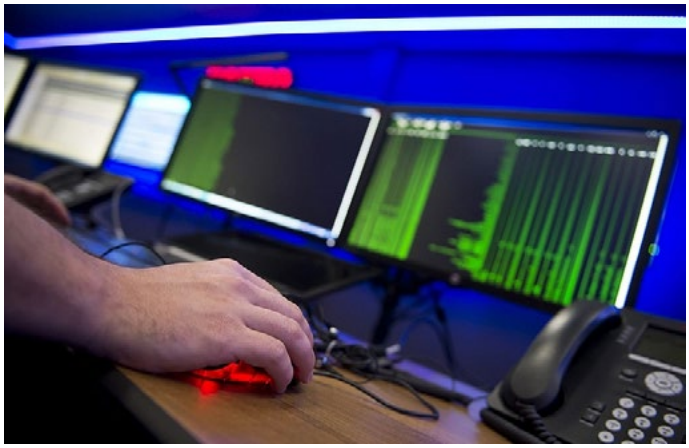
می‌توان گفت که دست کم می‌بایست همه‌ی اطلاعات حساس را به‌طور پیش‌فرض رمزگذاری کرد. کنترل شدیدی باید در نظر گرفته شود تا تضمین شود که فقط کارکنان مجاز می‌توانند به این اطلاعات دسترسی پیدا کنند.

این‌که چه کسی به کدام پرونده دسترسی دارد موضوعی است که بایست به‌طور مداوم بررسی شود تا اطمینان حاصل شود که هیچ نفوذی صورت نگرفته است.

بخش‌های مختلف باید امکان به اشتراک گذاری پرونده‌ها را با کانال‌های غیرمجازی همچون سامانه‌های عامل ابری غیرممکن سازند.

مدیریت امنیت

بازداشت عاملان نفوذ به جی‌پی‌مورگان در مسکو



جاشوا ساموئل هارون، ۳۲ ساله، یک شهروند آمریکایی مظنون به چندین نفوذ گسترده است؛ وی در می ۲۰۱۶ توسط مقامات روسیه بازداشت شد، دستگیری هارون در پی نقض قوانین ویزا توسط وی رخ داد.

مقامات آمریکایی، هارون و دو اسرائیلی را در تابستان ۲۰۱۵ به اتهام نفوذ و سرقت اطلاعات از ۱۲ شرکت بین‌المللی از جمله ۱۰ مؤسسه‌ی مالی از سال ۲۰۰۷ تا ۲۰۱۴، تحت تعقیب قانونی قرار داده‌اند.

فهرست شرکت‌هایی که نقض اطلاعات در آن‌ها به تأیید رسیده شامل جی‌پی‌مورگان چیس، وال‌استریت ژورنال، Scottrade، TD Ameritrade و ... می‌باشد.

هم‌دستان هارون در سال ۲۰۱۵ در اسرائیل دستگیر شدند

مقامات ایالات متحده گفتند که هارون و دو اسرائیلی از آسیب‌پذیری Heartbleed برای نفوذ به کارگزارهای این شرکت‌ها و سرقت اطلاعات مالی بیش از ۱۰۰ میلیون کاربر سوءاستفاده کرده‌اند.

یک ماه پس از آن‌که مقامات آمریکایی این سه تن را متهم معرفی کردند، مقامات رژیم صهیونیستی دو مظنون اسرائیلی به نام‌های گری شالون و زیو اورنستین را دستگیر و تحویل دادند.

به گزارش بلومبرگ، هارون با سفر به اوکراین و پس از آن روسیه در سال ۲۰۱۵ میلادی از دست قانون ایالت متحده گریخته است؛ این اتفاق ۲ ماه قبل از آن رخ داد که مقامات آمریکایی رسماً اتهامات وی را علنی سازند.

هارون بعد از نقض قوانین روادید دستگیر شد

هارون و همسر اسرائیلی وی، از آن زمان در مسکو زندگی می‌کردند و این قضیه از دید محققان آمریکایی مخفی مانده بود.

پلیس روسیه هارون را در می امسال و در پی نقض قوانین روادید این کشور از سوی وی دستگیر نمود. روسیه حکم کرده که مهاجران بایست این کشور را ترک کرده و پس از شش ماه مجدداً بازگردند.

هارون از زمان ورودش به روسیه با یک ویزای باطل‌شده در مسکو زندگی می‌کرد.

هارون به دنبال پناهندگی سیاسی

مقاماتی که هارون را بازداشت کرده‌اند، وی را به خاطر نقض قوانین روادید ۵هزار روبل معادل ۸۰ دلار جریمه کرده‌اند، و قاضی پرونده دستور اخراج او از روسیه را صادر کرده است.

هارون برای جلوگیری از این‌که به آمریکا فرستاده شود، به دنبال پناهندگی سیاسی است؛ البته قاضی پرونده این درخواست هارون را در تابستان گذشته رد کرده است.

در این میان هارون به یک درخواست تجدید نظر واصل شده تا اخراج خود را به تأخیر بیاندازد.

بلومبرگ به نقل از یک منبع داخلی این کشور گفت که مقامات روسی سعی داشته‌اند هارون را به خاطر یک قانون نامشخص «متقابل» مبادله کنند، که به احتمال زیاد به سود این دو کشور است، که این دو کشور هیچ معاهده‌ی استرداد متقابلی ندارند.

هارون از ماه می تاکنون در یک مرکز ویژه که روسیه برای مهاجران غیرقانونی در نظر گرفته زندگی می‌کند. پس از آن‌که جوابیه‌ی درخواست پناهندگی وی صادر شد، هارون می‌تواند به هر کشوری که انتخاب کند سفر نماید.

هارون و یکی از دوستان هم‌دانشگاهی وی به نام آنتونی مورجیو، در زمان جوانی خود بارها به روسیه سفر کرده‌اند. مقامات این کشور تصور می‌کنند که ممکن است یک نفوذگر روسی به آن‌ها کمک کرده باشد. مورجیو پس از روشن شدن چندین اتهامش در بازداشت به سر می‌برد؛ اتهامات وی سوءاستفاده از یک اتحادیه‌ی اعتباری در نیوجرسی برای پول‌شویی در قالب بیت‌کوین است.

مدیریت امنیت

دومین نفوذ به بانک‌های متصل به سوئیفت

دومین گروه از نفوذگران سایبری ملقب به Odinaff توانسته به سامانه‌ی سوئیفت نفوذ کند.

ظاهراً گروه Odinaff از روشی مشابه با روش نفوذگرانی استفاده می‌کند که موفق شده است در اوایل این سال میلادی ۸۱ میلیون دلار را بانک مرکزی بنگلادش به سرقت ببرد.

به نظر می‌رسد که حملات وابسته به تروجان Odinaff و ابزارهای مرتبط با آن در ژانویه‌ی سال ۲۰۱۶ شروع شده باشد. این حملات محدوده‌ی گسترده‌ای از مناطق جغرافیایی را درگیر خود کرده‌اند؛ در این میان آمریکا بیشتر از سایر کشورها هدف این حملات بوده، پس از آن هنگ‌کنگ، استرالیا، انگلستان و اوکراین قرار دارند.

میزان موفقیت این حملات هنوز مشخص نیست؛ همچنین از مقدار پولی که نفوذگران پشت این حملات به جیب زده‌اند اطلاعی در دست نیست.

هدف این حملات بیشتر مؤسسات مالی و بانک‌ها بوده است. بدافزار مربوط به این حمله از طریق رایانامه‌های اسپیرفیشینگ منتشر شده است، که بسیاری از این رایانامه‌ها حاوی ماکروهای مخرب بوده‌اند.

بایگانی‌های RAR مورد حفاظت با گذرواژه نیز گونه‌ی دیگری از حقه برای فریب دادن کاربران از همه‌جا بی‌خبر می‌باشند.

بخشی از مؤلفه‌های مخرب Odinaff از طریق باتنت در ماشین‌هایی وارد شده‌اند که در حال حاضر آلوده هستند. شرکت امنیتی سیمنتک توانسته شواهدی از وجود یک ابزار را پیدا کند که قادر است گزارش‌های انتقال مشتری‌های سوئیفت را دستکاری کند و رایانه‌ها را به منظور پنهان ساختن اثر هرگونه فعالیت احتمالی پاک نماید.

در این حملات Odinaff پیوندهایی به گروه Carbanak را منتشر می‌کند؛ فعالیت‌های این گروه در اواخر سال ۲۰۱۴ میلادی کشف و افشا شد. Carbanak همچنین در حملات معروف علیه مؤسسات مالی استفاده شده و در یک رشته از حملات علیه بانک‌ها و نیز پایانه‌های فروش مورد استفاده قرار گرفته است.

سه آدرس IP فرماندهی و کنترل که به کمپین‌های سابقاً گزارش‌شده‌ی Carbanak مربوط هستند، در مورد Odinaff نیز رؤیت شده‌اند. دلیل این تشابه شاید همکاری دو گروه مذکور با یکدیگر باشد.

کوین بوکک، استراتژیست ارشد Venafi در حوزه‌ی امنیت سایبری، می‌گوید: «این حملات به سوئیفت مانند سرقت از بانک به شیوه‌های ابتدایی آن هم در عصر دیجیتال است.»

«این یک تحول در حملات قدیمی است که بیشتر روی سرقت از مشتریان بانکی تمرکز دارد. پس از نخستین نفوذ موفقیت‌آمیز به سوئیفت، اصلاً جای تعجب وجود ندارد که چنین موضوعی مجدداً به سرخط خبرها برگردد؛ می‌توان گفت که اگر این اتفاق دیگر نیافتد همه‌ی ما متعجب خواهیم شد!»

مدیریت امنیت

پلیس لندن عاملان ورود بدافزار به ATMها را بازداشت کرد

پلیس لندن همچنان در جست‌وجوی مجرمانی است که بدافزاری را در دستگاه‌های خودپرداز این شهر نصب کرده‌اند، در این میان یک مرد رومانیایی مشکوک به دست داشتن در این جریان به انگلستان استرداد داده شده است.

امانوئل لیاهو در سال ۲۰۱۴ به توطئه‌چینی برای فریب اذهان عمومی و سرقت ۱,۵ میلیون یورو از دستگاه‌های خودپرداز شهر لندن متهم شده بود.

امانوئل عضو باندی بود که دو تن از اعضای دیگر آن به نام‌های گریگور پالادی و تئوفیل بورتوس در سال ۲۰۱۴ و ۲۰۱۵، به خاطر غارت دستگاه‌های خودپرداز آسیب‌پذیر به ترتیب به ۵ و ۷ سال زندان محکوم شدند.

اما دوعضو دیگر این گروه همچنان آزادانه فعالیت می کنند .

این گروه به دستگاه‌های خودپرداز راه پیدا کردند، به مؤلفه‌هایی برای بارگذاری بدافزار در دستگاه دسترسی یافتند، و به این ترتیب موفق شدند مقدار زیادی پول نقد را به جیب بزنند.

نکته‌ی جالب این است که این بدافزار در پایان کار خود را پاک می‌کند تا امکان هرگونه تجزیه و تحلیلی را از بین ببرد.

پلیس هرگز نتوانست به ماهیت بدافزار مورد استفاده در این حملات پی ببرد، از این رو جریان‌هایی پیدا شدند که طی آن‌ها بدافزارها در دستگاه‌های خودپرداز آسیب‌پذیر بارگذاری می‌شدند و در نتیجه نفوذگران دارای دسترسی از راه دور می‌توانستند محدودیت وضع‌شده برای میزان پول خروجی و سایر کنترل‌های امنیتی را دور بزنند.

متیو مونتفورد، بازرس تیم مبارزه با کلاه‌برداری لندن می‌گوید که پلیس رومانی در کمک به دستگیری مجرمان پشت پرده‌ی این جرایم بسیار فعالانه عمل کرده است. او گفت: «ما کار را با هم ادامه خواهیم داد تا مطمئن شویم که اعضای این باند مجرم هیچ جایی برای پنهان شدن ندارند.»

لیاهو در ۳۰ سپتامبر در دادگاه بدوی شهر لندن حاضر شد و تا ۲۸ اکتبر در بازداشت به سر برد.

تعداد پلیس‌هایی که به فعالیت‌های ضدکلاه‌برداری و سرکوب نفوذگران کلاه‌سیاه مشغول هستند در سال‌های اخیر افزایش یافته است تا به این طریق به تلاش‌های صورت‌گرفته برای مبارزه با جرایم بین‌الملل کمک شود.

مدیریت امنیت

برنده‌ی جایزه‌ی ۵۰هزار دلاری برای ارائه‌ی راه حل یافتن دستگاه‌های آسیب‌پذیر IoT باشید

اگر در مورد ناامنی اینترنت اشیاء نگران هستید، و دستی در برنامه‌نویسی دارید و از نحوه‌ی نفوذ به دستگاه‌های هوشمند خبر دارید، این فرصت را دارید که جایزه‌ی ۵۰هزار دلاری را برای کشف روش‌های غیرسنتی برای ایمن‌سازی اینترنت اشیاء از آن خود نمایید.

در دهه‌ی آینده بازار اینترنت اشیاء (IoT) گرم خواهد شد. در حال حاضر ۶,۵ تا ۸ میلیون دستگاه IoT متصل به اینترنت در سرتاسر جهان وجود دارد، و انتظار می‌رود که این عدد تا سال ۲۰۲۰ میلادی به ۵۰ میلیارد برسد.

اگرچه IoT زندگی بسیاری از کاربران را بهبود می‌بخشد، اما تعداد خطارت امنیتی مربوط به فقدان تدابیر امنیتی شدید و ساز و کار رمزگذاری نیز در این‌گونه دستگاه‌ها به‌طور فزاینده‌ای در حال افزایش است.

این افزایش در تعداد خطرات امنیتی منجر به گسترده‌تر شدن سطح حملات می‌شود، و نقاط ورودی بسیاری را در اختیار نفوذگران قرار می‌دهد تا به این طریق زندگی شما را دگرگون کنند.

همان‌طور که در خبرهای این وبگاه به اطلاع شما رسانیدم، ما به تازگی شاهد یک حمله‌ی انسداد سرویس توزیع‌شده علیه ارائه‌دهنده‌ی سرویس میزبانی فرانسوی OVH بوده‌ایم که سرعت وقوع آن بیش از ۱ ترابیت در ثانیه بوده است. این حمله توسط باتنتی از دستگاه‌های آلوده‌ی مبتنی بر اینترنت اشیاء ملقب به بدافزار Mirai رخ داده است.

به همین خاطر این تهدید برای اینترنت اشیاء گسترده بوده است، و محققان بایست همین امروز به فکر یافتن یک راه حل باشند و فردا برای این کار خیلی دیر است.

هم‌اکنون ما روش‌هایی همچون موتور جست‌وجوی Shodan و Censys را برای یافتن دستگاه‌های آسیب‌پذیر داریم. در حالی که Shodan به‌طور ویژه برای تعیین موقعیت مکانی هر دستگاهی طراحی شده که با بی‌دقتی به اینترنت وصل شده است، اما Censys یک روی‌کرد بسیار پیشرفته‌تر را برای پیدا کردن آسیب‌پذیری‌های داخل دستگاه‌ها از طریق پویش کل اینترنت به کار می‌گیرد.

با این حال شامل راه‌های خلاقانه برای کشف دستگاه‌های آسیب‌پذیر مبتنی بر اینترنت اشیاء شامل یک هواپیمای بدون سرنشین به همراه یک ابزار ردیابی است که قادر است داده‌ها را از دستگاه‌های متصل به اینترنت اشیاء شنود کند.

چالش: پیدا کردن راه‌هایی برای یافتن دستگاه‌ی IoT آسیب پذیر

حالا شرکت تحقیق و توسعه‌ی ناسودبر MITRE در پی یافتن راهی برای نظارت بر دستگاه‌ی IoT آسیب‌پذیر برای کمک به مدیران شبکه، محققان را برای ارائه‌ی ایده‌های جدید جهت شناسایی دستگاه‌های اینترنت اشیای جعلی در یک شبکه فراخوانی نموده است.

خبر خوب این‌که شما می‌توانید در ازای ایده‌ای که ارائه می‌دهید ۵۰هزار دلار به جیب بزنید. محققانی که موفق شوند روی‌کردهای غیرسنتی و نوینی را برای شناسایی دستگاه‌های IoT حین نظارت منفعلانه روی شبکه، و بدون نیاز به تغییر پروتکل‌ها و خروجی شبکه ارائه نمایند، می‌توانند مبلغی بالغ بر ۵۰هزار دلار را با خود به خانه ببرند!

آنچه که شرکت MITRE در کنار جایزه‌ی نقدی وعده داد است:

شناخت و توسعه.

داشتن فرصت برای ارتباط با سازمان‌های دولتی برای یافتن راه‌کارهای اینترنت اشیاء.

شانس کار با کارشناسان MITRE برای درک بهتر نیازهای دولت.

تیم اینترنت اشیای MITRE یک مدل از شبکه‌ی خانگی را ساخته که به عنوان یک بستر آزمایشی برای این چالش معرفی شده است. این شبکه‌ی خانگی قدرتمند شامل محدوده‌ی گسترده‌ای از دستگاه‌های مقرون‌به‌صرفه است که دارای ویژگی‌های اجرایی مختلفی هستند.

این چالش برای کارآفرینان فردی، تیم‌های دانشگاهی که به دنبال نمایش استعدادهای خود هستند و نیز شرکت‌های کوچکی تدارک دیده شده که قصد دارند در بازار اینترنت اشیاء خودی نشان بدهند.

زمان ثبت‌نام برای حضور در این چالش در حال حاضر شروع شده است، بنابراین اگر قصد شرکت دارید سریع وارد عمل شوید. این چالش در ابتدای نوامبر آغاز می‌شود و حدود شش هفته به طول خواهد انجامید، بنابراین همه‌ی شرکت‌کنندگان بایست یک راه‌کار منحصربه‌فرد، ساده و مقرون‌به‌صرفه را برای شناسایی دستگاه‌های IoT در این بازه‌ی زمانی کوتاه معرفی نمایند.

برنده‌ی این رقابت قبل از پایان دسامبر اعلام خواهد شد. بنابراین، اگر تصور می‌کنید از توانایی لازم برای یافتن راه حل مناسب این مسئله برخوردارید، پس منتظر چه چیزی هستید؟ همین امروز ثبت نام کنید.

مدیریت امنیت

محکومیت دو عضو گروه Dridex به ۱۲ سال زندان

یک دادگاه انگلیسی دو نفر از اعضای گروه Didex را هریک به ۱۲ سال زندان محکوم کرده است. آن‌ها متهم هستند که از طریق بدافزار Dridex بیش از ۲.۵ میلیون یورو (۳.۲ میلیون دلار) را به دست آورده‌اند.

این دو مجرم پاول گینکوتا ۳۲ ساله و یون تورسان ۳۵ ساله، هر دو اصالتاً از جمهوری مولداوی بوده اما به انگلستان سفر کرده بودند.

در بین سال‌های ۲۰۱۳ تا ۲۰۱۵، برای مدت دو سال گینکوتا و تورسان به‌عنوان قاطر پول ایفای نقش می‌کرده‌اند. قاطر پول اصطلاحی است که برای توصیف مجرمان فعال در پول‌شویی به کار می‌رود. این دو نیز در این سال‌ها به پول‌شویی مبالغ به سرقت رفته توسط گروه Dridex مشغول بوده‌اند و بدین ترتیب بخشی از این پول را از آن خود می‌کرده‌اند.

گروه Dridex دسترسی‌های لازم را برای این دو مجرم به حساب‌های بانکی مورد نفوذ واقع شده فراهم می‌کردند تا گینکوتا و تورسان بتوانند مبالغ مورد نظر را به حساب‌های تحت کنترل خود منتقل کنند. بدین ترتیب آن‌ها می‌توانستند اقدام به خرید کالای گران‌قیمت کرده، از طریق خودپرداز پول دریافت کرده و یا به بخش‌های مختلف گروه Dridex پول تزریق کنند.

به گزارش آژانس مبارزه با جرائم ملی انگلیس این دو نفر کنترل بیش از ۲۲۰ حساب بانکی را در اختیار داشته‌اند.

مقامات انگلیسی در فوریه ۲۰۱۵ در حالی به این دو نفر مظنون شدند که اسناد هویتی‌شان جعلی بود. پلیس این اسناد را مشکوک دانسته و پس از بررسی آپارتمان محل زندگی آن‌ها، توانست اسناد جعلی دیگری را به همراه دستگاه‌های الکترونیکی مختلف ازجمله لپ‌تاپی که برای دسترسی به حساب‌های مورد نفوذ واقع شده استفاده می‌شد کشف و ضبط کند. با مدارک به دست آمده این دو نفر مجرم شناخته شده و هریک به ۱۲ سال زندان محکوم شدند.

گینکوتا و تورسان سرکرده‌های گروه کلاهبرداری Dridex نبودند بلکه برعکس کم‌رنگ‌ترین نقش را در این گروه مجرمانه بازی می‌کرده‌اند. گروه Dridex به‌راحتی می‌تواند جای این دو نفر را با افراد دیگر پر کند. افراد مشابه دیگری در نقش قاطران پول در انجمن‌های نفوذ زیرزمینی ایفای نقش می‌کنند. در ماه جولای نیز مقامات انگلیسی اعلام کره بودند ۵ فرد روسی‌تبار را که در همین نقش ظاهر می‌شده‌اند دستگیر و به زندان انداخته‌اند.

مدیریت امنیت

سرقت اطلاعات مربوط به ۵۸ میلیون کاربر در یک ارائه‌دهنده خدمات ذخیره‌سازی

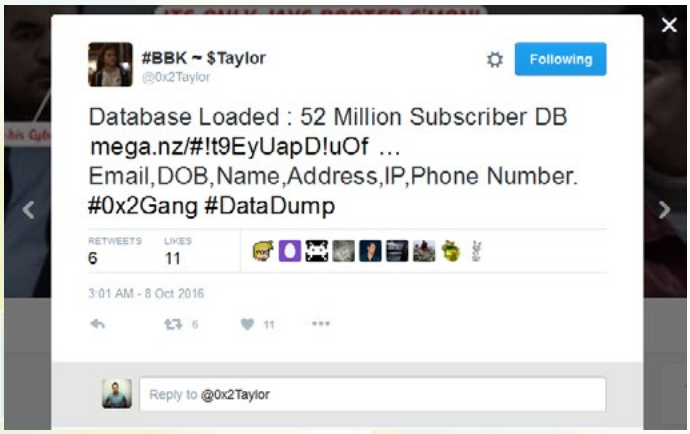
خبرها حاکی از آن است که یک پایگاه داده ناامن به حداقل یک نفوذگر امکان داده است تا داده‌های کارگزار شرکت Modern Business Solutions را به سرقت ببرد. این شرکت خدمات ذخیره‌سازی داده و راهکارهای میزبانی پایگاه داده را ارائه می‌کند.

این شرکت هنوز بیانیه رسمی درباره این رخداد منتشر نکرده است اما پایگاه داده مذکور را در برابر دسترسی‌های خارجی امن کرده است.

نفوذگری که مسئول این رخنه است در توییتر با حساب 0x2Taylor فعالیت دارد. این نفوذگر پس از آن‌که این سرویس میزبانی پرونده پایگاه داده را حذف کرد تابه‌حال 3 مرتبه اقدام به انتشار داده‌های به سرقت‌رفته بر روی حساب‌کاربری توییتر خود کرده است.

شرکت امنیت سایبری (RBS) Risk Based Security داده‌های مورد نفوذ واقع‌شده را تحلیل و تائید کرده است که این داده‌ها متعلق به پایگاه داده MongoDB بوده که ۵۸ میلیون کاربر داشته است.MongoDB یک پایگاه داده‌های سند-گرای متن‌باز، کارا، مقیاس‌پذیر است که در دسته پایگاه داده‌های NoSQL قرار گرفته و در زبان برنامه‌نویسی سی++ نوشته شده است. این پایگاه داده به جای اینکه همانند پایگاه‌های داده‌ی رابطه‌ای کلاسیک داده‌ها را در جداول ذخیره کند، داده‌های ساختاریافته را در اسنادی با قالبی شبیه به JSON (در MongoDB این قالب را BSON می‌نامند) ذخیره‌سازی می‌کند و بدین ترتیب یکپارچه‌سازی داده‌ها را در برخی برنامه‌های کاربردی آسان‌تر و سریع‌تر می‌کند.

داده‌های به سرقت‌رفته از این پایگاه داده شامل نام کامل کاربران، آدرس‌های IP، تاریخ تولد، آدرس‌های رایانامه و موقعیت شغلی است. در مکالمات خصوصی انجام شده با 0x2Taylor، او تأیید کرده است که داده‌های را از یک پایگاه داده MogoDB بارگیری کرده است که به‌صورت برخط در دسترس بوده است. او هم‌چنین گفته یکی از دوستانش این پایگاه داده را با استفاده از موتور جستجوی Shodan کشف کرده و آدرس IP آن را بدون اطلاع شرکت مربوطه، به‌صورت برخط منتشر کرده است.



شرکت امنیتی RBS جداولی از پایگاه‌داده را که با «_hw»

آغاز می‌شد تحلیل کرده است. محصول اصلی MBS بستر مدیریت داده‌ای مبتنی بر فضای ابری با نام Hardwell Data است. البته MBS تأیید نکرده است که داده‌های ناامن ذخیره شده متعلق به مشتریان Hardwell Data بوده‌اند.

RBS هم‌چنین گفته است پیش از این‌که MBS پایگاه داده مورد نفوذ را امن کند، 0x2Taylor تصویری را در تحلیل‌هایش منتشر کرده است که فاش می‌کند او موفق شده است جداولی از یک پایگاه داده دیگر را پیدا کند که نزدیک به ۲۵۸ میلیون کاربر دارد.

گروه امنیتی RBS در تکمیل توضیحات خود می‌گویند: «تا به این لحظه ۲۰۲۸ مورد نفوذ داده، امسال به‌صورت عمومی رخ داده است که بیش از ۲.۲ میلیارد رکورد اطلاعاتی را در معرض خطر قرار داده‌اند. درحالی که این ۲.۲ میلیارد مورد، عدد بزرگی محسوب می‌شود، تحقیقات RBS نشان می‌دهد که ۵۵ درصد این رخنه‌ها در نیمه ابتدایی سال ۲۰۱۶ رخ داده و تنها ۱۰ هزار رکورد را منتشر کرده‌اند. متأسفانه برخی از این رخنه‌های عظیم در اثر تنظیمات ناصحیح پایگاه داده رخ داده‌اند.»

مدیریت امنیت

۳ اولویت مهم در امنیت اطلاعات

شرکت‌ها دائماً در حال هک شدن هستند بدون اینکه مجازاتی برای مجرمان وجود داشته باشد بخاطر اینکه ما اصول اساسی و پایه‌ای را انجام نمی‌دهیم. این‌ها به این دلیل نیست که ما فاقد هوشمندی موجود در تهدیدها هستیم و APT ها وجود دارند.

این‌ها همه بخاطر این است که ما در ایستادن، راه رفتن و دویدن شکست می‌خوریم. ما در مرحله‌ی ایستادن درگیر پیچیدگی‌های موانع و پرش‌های بلند شده‌ایم. این اولین جلسه‌ی ما در کلاس کاراته است و ما برای دست یافتن به کمربند سیاه و سفید تلاش می‌کنیم.

اگر شما دوست، مشتری و یا هرکس دیگری در دنیای امنیت اطلاعات دارید، این 3 موردی که در ادامه بیان می‌کنیم، مهم‌ترین چیزی است که باید بر روی آن متمرکز شوید.

- کنترل دارایی
- مدیریت وصله‌ها
- ترافیک خروجی

کنترل دارایی:

وقتی نمی‌دانید چه دارایی‌هایی دارید، هیچ‌وقت نمی‌توانید از آن‌ها دفاع کنید.

– تمام دارایی‌های خود را پیدا کنید.
– آن‌ها را در یک فهرست قرار دهید.
– مرتب این فهرست را به‌روزرسانی کنید.
– همواره به چشم‌انداز IT آن‌ها توجه کنید.

مدیریت وصله‌ها:

اگر آسیب‌پذیری‌های موجود را وصله نکرده‌اید، وصله کردن آن‌ها در اولویت قرار دارد.

– با استفاده از فهرست دارایی‌ها، آن‌ها را وصله نمایید.
– سامانه عامل خود را به نسخه‌ی جدید به‌روزرسانی کنید.
– برنامه‌های کاربردی را به آخرین نسخه به‌روزرسانی کنید.
– اگر نمی‌توانید برنامه‌های خود را به‌روز رسانی کنید، از برنامه‌ها تحت عنوان سرویس استفاده نمایید.

ترافیک خروجی:

ترافیک خروجی، پنجره‌ای برای در معرض خطر قرار گرفتن است.

– ترافیک DNS خود را کنترل کنید.
– از فهرست‌های سیاه به سمت فهرست سفید حرکت دهید.
– ارتباطات سامانه‌ی خود را با میزبان‌هایی که مخرب شناسایی شده‌اند، متوقف کنید.
– از یک IPS/IDS برای تشخیص ترافیک مخرب مربوط به

ارتباطات خروجی استفاده کنید.

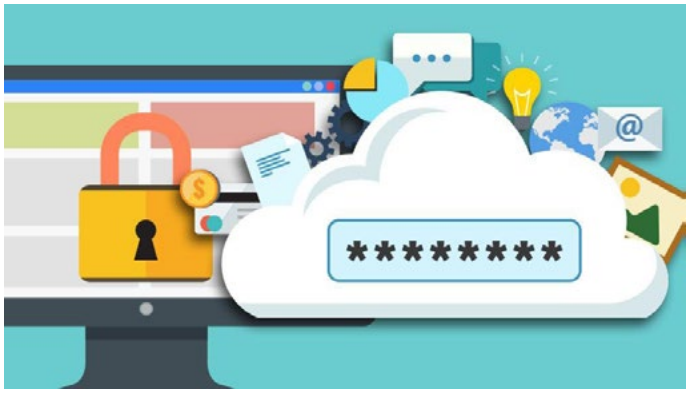
این مراحل اورژانسی و در هر رده بسیار اساسی و مهم هستند. اما ترتیب اجرای این موارد بستگی به نوع سازمان شما دارد. ولی مواردی که گفته شد به نوعی اصول زیر را اعمال می‌کنند:

- حفاظت از نقطه‌ی انتهایی
- ثبت رویداد نام‌ها و نظارت و کنترل
- پاسخ به رویداد

حال که این اولویت‌های اساسی ذکر شد، به دنبال موارد 4 و 5 و 6 نگردید و روی همین اولویت‌های 1، 2 و 3 تمرکز کنید. بایستید، راه بروید و بدوید.

مدیریت امنیت

آمازون در اقدام پیشگیرانه‌ای گذرواژه‌ی مشتریان را بازنشانی می‌کند



شرکت آمازون پس از اینکه متوجه شد گذرواژه‌ی کاربرانش ممکن است در سرویس‌های برخط دیگر نیز مورد استفاده قرار گرفته باشد، از مشتریان خواست تا گذرواژه‌های خود را بازنشانی کنند.

آمازون طی رایانامه‌ای مشتریان خود را مطلع کرده تا گذرواژه‌های خود را تغییر دهند. آمازون مدعی شده در طول یک نظارت معمولی، فهرستی از رایانامه و گذرواژه‌ها را به‌طور برخط کشف کرده و اقدامات پیشگیرانه بر روی آن‌ها را آغاز کرده است. همچنین این شرکت اظهار کرده که این گذرواژه‌ها هیچ ارتباطی به آمازون ندارند.

با مشاهده‌ی نقض داده‌های عظیمی که در طول این چند ماه مشاهده شده، خیلی عجیب نیست که آمازون در یک اقدام پیشگیرانه دست به چنین عملی زده باشد. سایر سرویس‌های برخط نیز اینترنت را برای مشاهده‌ی نام کاربری و گذرواژه‌ها نقض‌شده بررسی می‌کنند تا مطمئن شوند تا کاربران آن‌ها از این گذرواژه‌ها استفاده نمی‌کنند.برخی از نفوذهای مهمی که امسال کشف شد عبارتند از دراپ‌باکس (68 حساب کاربری تحت تأثیر قرار گرفته)، لینکدین (168 میلیون)، مای‌اسپیس (360 میلیون)، تامبلر(65 میلیون) و وی‌کی (170 میلیون). این فهرست با نقض داده‌ی نزدیک به 500 میلیون کاربر یاهو در ماه گذشته تکمیل شد.

چیزی که آمازون آشکار نکرده این است که این نام کاربری/گذرواژه‌ها برای چه مدت زمانی بوده و چه بخشی را مدیریت کرده تا این اطلاعات را بدست آورد. هرچند که چندین پایگاه داده‌ی مربوط به کاربران به‌طور برخط منتشر شده که بدون شک فرصت‌های زیادی را برای بررسی آمازون فراهم آورده است.

در رایانامه‌ای که آمازون به مشریان ارسال کرده از آنان خواسته که نه تنها گذرواژه‌ی جدید انتخاب کنند که این گذرواژه با آنچه که قبلاً در این وب‌گاه استفاده کرده بودند، متفاوت باشد بلکه توجه کنند که این گذرواژه در وب‌گاه دیگری نیز استفاده نشده باشد. به عبارت دیگر برای هر سرویس برخطی که کاربر استفاده می‌کند، باید یک گذرواژه‌ی منحصربفرد داشته باشد.

کاربرانی که تحت تأثیر قرار گرفته‌اند باید تغییر گذرواژه‌ی خود در سایر سرویس‌های برخط را نیز بررسی کنند تا مطمئن شوند که در امنیت کامل هستند. همچنین بهتر است که کاربران از یک برنامه‌ی مدیریت گذرواژه استفاده کنند که مدیریت چندین حساب کاربری با گذرواژه‌ی منحصربفرد را به کار بسیار راحتی تبدیل می‌کند.

پس از اینکه دور اول نقض داده‌های عظیم رخ داد، حملاتی که به جزئیات اطلاعات نقض‌شده‌ی کاربران نفوذ می‌کند، اوایل امسال مشاهده شده است. در این حملات حساب‌های کاربری گیت‌هاب هدف قرار گرفت و سرویس‌های برخط تصمیم گرفتند گذرواژه‌های کاربرانی که حساب‌های آن‌ها در معرض خطر قرار گرفته بود را بازنشانی کنند.

مدیریت امنیت

مرکز صدور گواهی WoSign، بدنبال بخشیده شدن توسط مرورگرها

در پی پیشنهاد فایرفاکس که حداقل یکسال گواهی‌نامه‌های مرکز WoSign را تحریم کرد و بدنبال آن اپل که تصمیم گرفت گواهی‌نامه‌های آن را باطل کند، این شرکت با اقدامات جدی و مهمی ظاهر می‌شود تا توسط مرورگرهای مهم بخشوده شود.

موزیلا هفته گذشته با نمایندگان StartCom، Qihoo 360 و WoSign بزرگ‌ترین سهام‌دار ملاقات کرد تا در مورد این مسائل بحث کند. بعد از این جلسه، WoSign گزارشی منتشر کرد که بعد از این حادثه تصمیم دارد برخی تغییرات در بخش رهبری، فرآیندهای عملیاتی و فناوری اعمال کند.

Qihoo 360 می‌خواهد به‌طور کامل در زمینه‌ی عملیاتی و تکنولوژی از WoSign و StartCom جدا شود و از فروشندگان مرورگرها خواسته تا هر شرکت را به‌طور جداگانه قضاوت کنند. ریچارد وانگ، مدیر عامل شرکت WoSign که صدور گواهی‌هایی که قبلاً به‌روز و معتبر بوده است (که جدی‌ترین مشکل مطرح شده بود) را تائید کرد و از تمامی وظایف خود برکنار شد.

StartCom بطور مستقیم به Qihoo 360 گزارش خواهد داد با نظر به اینکه Xiaosheng Tan به عنوان رئیس و Inigo Barreira به عنوان مدیرعامل منصوب شدند. به علاوه هر دو شرکت گواهی‌های خود را در بخش ثبت رویداد شفافیت گواهی (CT) اضافه خواهند کرد.

WoSign در گزارش رخداد خود نوشت: «ما کاملاً قبول داریم که حفظ امنیت اینترنت برای تمامی سهامداران در زمینه ی CA بسیار مهم است. از موزیلا بسیار ممنونیم که مصلحت و مزایای مشترکان WoSign و StartCom را بررسی کرده است. ما از فایرفاکس قدردانی می کنیم. بسیاری از مشتریان در چین فهمیدند که مهم است که از یک CA داخلی برای اهداف امنیتی استفاده کنند.»

اکنون توپ در زمین موزیلا است. این شرکت ممنوعیت حداقل یکساله را برای دو شرکت WoSign و StartCom پیشنهاد داد. این پیشنهاد پس از اینکه موزیلا فهمید بیش از دوازده مورد اعم از ارائه‌ی گواهی‌های معبر قبلی از 1 ژانویه‌ی 2016 مربوط به این دو شرکت بوده است، ارائه شد.

در اواخر سپتامبر، اپل اعلام کرد قصد انتشار به‌روزرسانی‌های امنیتی برای iOS و OS X دارد که این محصولات دیگر به هیچ گواهی صادر شده توسط مرکز صدور گواهی WoSign گواهی SSL رایگان و CA میانی G2 اعتماد نخواهد کرد. این شرکت اشاره کرد که WoSign ارتباط با StartCom و Comodo را برای ایجاد اعتماد بکار برده است چرا که هیچ گواهی ریشه در فروشگاه اعتماد اپل ندارد.

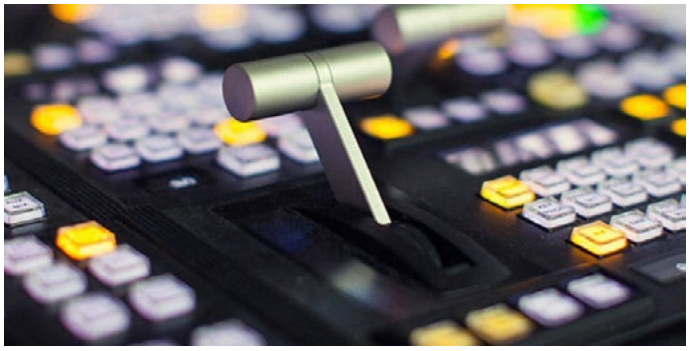
گوگل و مایکروسافت هنوز در مورد این مسئله نظری نداده‌اند. بسیاری از شرکت‌ها و بویژه گوگل زمانی که رفتار نادرستی از CA ها مشاهده کنند، خیلی در این خصوص بخششی نخواهند داشت.

فصل سوم

امنیت سایبری

امنیت‌سایبری

مدیر آژانس بین‌المللی انرژی اتمی از یک نفوذ سایبری به نیروگاه‌های هسته‌ای خبر داد



مدیر آژانس بین‌المللی انرژی اتمی گفته است که از نفوذی موفقیت‌آمیز به یک نیروگاه هسته‌ای اطلاع دارد. خبر بدتر این‌که وی شاهد تلاش‌های صورت‌گرفته برای سرقت اورانیوم غنی‌شده بوده است.

روز دوشنبه یوکیا آمانو، مدیر این آژانس برای شرکت در یک سری جلسات به آلمان سفر کرد؛ جایی که یکی از خبرنگاران رویترز از زبان او شنید که سه یا چهار سال پیش حمله‌ای علیه یک نیروگاه صورت گرفته است و تأسیسات مورد نظر برخی از اقدام‌های احتیاطی لازم را انجام داده است.

ظاهراً این نیروگاه نیازی به تعطیل‌شدن نداشته است.

به گزارش خبرگزاری‌ها، آمانو گفته که از تلاش برای «قاچاق مقدار کمی اورانیوم غنی‌شده، در حدود سه یا چهار سال پیش، مطلع بوده که ممکن است از این مواد برای تولید بمب کثیف استفاده شود.»

اظهارات آمانو در وهله‌ی اول وحشتناک به نظر می‌رسد، اما شاید قضیه وقتی وحشتناک‌تر شود که به یاد افشای داستانی در ۲۰۱۳ بیافتیم، زمانی که کاشف به عمل آمد که نیروگاه‌های هسته‌ای کانادا کدی را اجرا می‌کنند که به‌طور ویژه برای مدل PDP-11 از رایانه‌های کوچکی تهیه شده برای دست کم ۳۰ سال آینده استفاده می‌شوند.

می‌بایست ضدبدافزارهایی برای این مشکل ارائه شود و یا کارشناسان امنیتی خبره‌ای وارد کار شوند که قسمت‌های داخلی این کد را درک می‌نمایند.

امنیت‌سایبری

کشف یک در پشتی که رمزگذاری دیفی-هلمن صدها میلیون پیام را تهدید می‌کند

سوی رمزگشایی این لگاریتم گسسته داشته باشند.
یکی از محققان دانشگاه ایالت پنسیلوانیا به نام نادیا هنینگر که در این تحقیق حضور داشته گفت: «ما نشان دادیم که یک سری اعداد اول داریم که امکان شکستن کلیدهای ۱۰۲۴ بیتی را به‌طور کامل میسر می‌سازند.»

محققان موفق به ابداع روشی شده‌اند که رمزگشایی را ممکن می‌سازد.
کارشناسان توانسته‌اند راهی را پیدا کنند تا به وسیله‌ی آن در پشتی‌هایی را در کلیدهای رمزنگاری جاسازی نمایند؛ از این کلیدها برای محافظت از وب‌گاه‌ها، شبکه‌های خصوصی مجازی، و کارگزارهای اینترنتی استفاده می‌شود.
محققان دو ماه تمام ۳۰۰۰ پردازنده را به کار گرفتند تا به این موفقیت دست پیدا نمایند.
نفوذگران با تزریق این در پشتی غیرقابل کشف در کلیدهای ۱۰۲۴ بیتی مورد استفاده در تبادل کلید دیفی-هلمن توانستند صدها میلیون پیام متعلق به ارتباطات رمزشده را رمزگشایی نمایند، همچنین خود را به عنوان صاحبان این کلیدها جا بزنند.
زمانی تصور می‌شد که این رمزگذاری غیرقابل نفوذ است، چرا که از اعداد اول بزرگ در آن استفاده می‌شود، اما محققان یک عدد اول ویژه را ساختند که این روند را ساده‌تر می‌کند.
بدین معنا که آن دست از عاملانی که به دنبال رمزگشایی ارتباطات هستند در حال حاضر ممکن است راهی به

امنیت‌سایبری

کمک چند میلیون دلاری سنگاپور برای بهبود امنیت اطلاعات آسه‌آن

سنگاپور حدود ۷٫۲ میلیون دلار را تقدیم صندوق آسه‌آن نمود تا به این طریق به امنیت اطلاعات این انجمن کمکی کرده باشد.

به گفته‌ی رسانه‌های این کشور، این پول صرف منابع، تخصص و آموزش شده است.

ایده‌ی این برنامه متعلق به وزیر ارتباطات و اطلاعات سنگاپور، دکتر یاکوب ابراهیم بوده است؛ وی در کنفرانس وزرای آسه‌آن در مورد امنیت سایبری در تاریخ ۱۱ اکتبر از این تصمیم صحبت کرده است.

قرار است که این مبلغ طی پنج سال برای فعالیت‌هایی همچون کارگاه‌های آموزشی و سمینارها مصرف شود؛ همچنین قرار است کارشناسان فنی را با افسران حوزه‌ی سیاست، دیپلمات‌ها و دادستان‌های آسه‌آن گرد هم جمع کند.

به استناد جاکارتا پست و استریتس تایمز، دکتر ابراهیم گفته که دولت‌های منطقه‌ی آسه‌آن مقابل تهدیدهایی همچون جرایم سایبری، جاسوسی، و سایر فعالیت‌های مخرب آسیب‌پذیر هستند.

مطالعات صورت‌گرفته در خارج از آسیا گفته‌های وی را تأیید می‌کند. در ماه آگوست، مندینت نخستین مطالعه‌ی خود راجع به این منطقه‌ی جغرافیایی را منتشر کرد؛ یافته‌های مندینت حاکی از آن بود که کسب و کار در جنوب شرق آسیا بدون توجه به مقوله‌ی امنیت پیش می‌رود. در این گزارش مثلاً آمده است که شرکت‌های این منطقه نمی‌دانند که چگونه بایست از شبکه‌ها مقابل نفوذ مهاجمان سایبری دفاع کنند و اطلاع ندارند که اولین کاری که بایست پس از یک نفوذ انجام دهند چیست.

امنیت‌سایبری

کمک چند میلیون دلاری سنگاپور برای بهبود امنیت اطلاعات آسه‌آن

سنگاپور حدود ۷,۲ میلیون دلار را تقدیم صندوق آسه‌آن نمود تا به این طریق به امنیت اطلاعات این انجمن کمکی کرده باشد.

به گفته‌ی رسانه‌های این کشور، این پول صرف منابع، تخصص و آموزش شده است.

ایده‌ی این برنامه متعلق به وزیر ارتباطات و اطلاعات سنگاپور، دکتر یاکوب ابراهیم بوده است؛ وی در کنفرانس وزرای آسه‌آن در مورد امنیت سایبری در تاریخ ۱۱ اکتبر از این تصمیم صحبت کرده است.

قرار است که این مبلغ طی پنج سال برای فعالیت‌هایی همچون کارگاه‌های آموزشی و سمینارها مصرف شود؛ همچنین قرار است کارشناسان فنی را با افسران حوزه‌ی سیاست، دیپلمات‌ها و دادستان‌های آسه‌آن گرد هم جمع کند.

به استناد جاکارتا پست و استریتس تایمز، دکتر ابراهیم گفته که دولت‌های منطقه‌ی آسه‌آن مقابل تهدیدهایی همچون جرایم سایبری، جاسوسی، و سایر فعالیت‌های مخرب آسیب‌پذیر هستند.

مطالعات صورت‌گرفته در خارج از آسیا گفته‌های وی را تأیید می‌کند. در ماه آگوست، مندینت نخستین مطالعه‌ی خود راجع به این منطقه‌ی جغرافیایی را منتشر کرد؛ یافته‌های مندینت حاکی از آن بود که کسب و کار در جنوب شرق آسیا بدون توجه به مقوله‌ی امنیت پیش می‌رود. در این گزارش مثلاً آمده است که شرکت‌های این منطقه نمی‌دانند که چگونه بایست از شبکه‌ها مقابل نفوذ مهاجمان سایبری دفاع کنند و اطلاع ندارند که اولین کاری که بایست پس از یک نفوذ انجام دهند چیست.

امنیت‌سایبری

مراکز تماس هندی ۷۵ میلیون دلار را با فریب شهروندان آمریکایی به چنگ آوردند

پلیس هند سه مرکز تماس را تعطیل کرده است؛ این مراکز تماس در منطقه‌ی تانه‌ی بمبئی مستقر هستند، به دنبال این ماجرا ۷۰ مظنون دستگیر شده‌اند و ظاهراً پلیس این کشور به ۶۳۰ نفر دیگر هم مشکوک است.

مقامات هند می‌گویند که این مراکز تماس در پشت پرده‌ی یک سری کلاه‌برداری مالی قرار داشته‌اند که شهروندان آمریکایی راه هدف قرار داده و بیش از ۷۵ میلیون دلار را از این راه به جیب زده‌اند.

متصدی‌های مراکز تماس که خود را به عنوان نماینده‌ی سرویس درآمد داخلی آمریکا جا زده‌اند، با شهروندان آمریکایی تماس گرفته و خود را نماینده‌ی مالیاتی ایالات متحده برای سرویس درآمد داخلی این کشور (IRS) معرفی کرده‌اند.

این تماس‌گیرندگان از یک لهجه‌ی آمریکایی غلیظ برخوردار بودند، از فن‌آوری VoIP برای مخفی‌سازی موقعیت مکانی خود بهره گرفتند، و به اهداف خود گفتند که آن‌ها (اهداف) در مورد پرداخت مالیات خود قصور کرده‌اند. این تماس‌گیرنده‌ها قربانی‌ها را با اتهام‌های رسمی، دستگیری یا جریمه‌های سنگین تهدید کرده‌اند.

کلاه‌برداران در ابتدا مبالغ هنگفتی را از قربانیان درخواست کرده‌اند، اما در ادامه این مبالغ را کاهش داده‌اند.

نرخ موفقیت این مراکز تماس ۵٪ بوده است

پلیس می‌گوید یک مورد از هر ۲۰ قربانی در نهایت حاضر به پرداخت مبلغ درخواستی شده است، به این ترتیب هر سه مرکز تماس روی هم رفته بین ۱۵۰ تا ۲۲۵ هزار دلار در روز درآمد داشته‌اند.

مقامات آمریکایی با همتایان هندی خود تماس گرفته‌اند تا اطلاعات بیشتری را در مورد این باند به دست بیاورند؛ ظاهراً اعضای این باند آمریکایی بوده‌اند. این اعضای آمریکایی تا قبل از شناسایی حدود ۳۰٪ از عملیات خود را پیش برده بودند.

Times of India می‌گوید که پلیس در دستگیری صاحبان این مراکز تماس ناموفق بوده است. این نشریه خاطرنشان کرد که پلیس هند از یک کارمند ناراضی اسبق مرکز تماس انعام دریافت کرده است.

محققان بر این باورند که این سه مرکز تماس عامل حمله، بخشی از یک شبکه‌ی بزرگ‌تر هستند. متصدی‌های این مراکز همگی در خانه آموزش دیده بودند.

انگلستان و استرالیا نیز ممکن است هدف حمله قرار گرفته باشند

تحقیقات هنوز هم ادامه دارد، و مقامات عقیده دارند که پس از بررسی شواهد می‌توانند بازداشت‌های بعدی را نیز ترتیب دهند.

مقامات گفته‌اند که ۸۵۲ هارد دیسک، کارگزارهای مدرن امروزی، DVRها، لپ‌تاپ و سایر تجهیزات را کشف و

ضبط کرده‌اند. ارزش این تجهیزات مصادره‌شده بالغ بر ۱۵۰هزار دلار می‌باشد.

این حمله در روز یکشنبه چهار اکتبر ۲۰۱۶ رخ داد. پلیس هند تصور می‌کند که ممکن است استرالیا و انگلستان هم جزء قربانی‌ها باشند.

امنیت‌سایبری

ساخت ابزار سری یاهو برای پویش محتوای رایانامه‌ها به دستور آژانس امنیت ملی آمریکا

کاربران کماکان درگیر نقض داده‌ی عظیم یاهو هستند که باعث شد ۱ میلیارد حساب کاربری یاهو افشا شود؛ حال خبر بد تکان‌دهنده‌ی دیگری راجع به این شرکت مطرح به بیرون درز کرده که ذهن کاربران را متوجه خود ساخت است؛

ممکن است یاهو داده‌های شخصی شما را در صورت نیاز به دست آژانس امنیت ملی آمریکا برساند.

بنا به گزارش رویترز یاهو یک نرم‌افزار سفارشی را تدارک دیده است که به‌صورت مخفیانه تمامی رایانامه‌های کاربران را برای به دست آوردن اطلاعات خاصی پویش می‌کند که از سوی مقامات اطلاعاتی آمریکا ارائه شده‌اند.

این ابزار در سال ۲۰۱۵ و پس از حکم مخفی دادگاه آمریکا برای پویش صدها میلیون حساب رایانامه‌ی یاهو به دستور NSA یا FBI، ایجاد شد؛ این اطلاعات از سه منبع جداگانه که با این موضوع سر و کار داشته‌اند نقل شده است.

به گفته‌ی برخی از کارشناسان، این اولین بار است که این شرکت اینترنتی آمریکایی با چنین تقاضای گسترده‌ای از سوی یک سازمان جاسوسی برای جست‌وجوی تمام رایانامه‌های ورودی، بررسی رایانامه‌های ذخیره‌شده و یا پویش تعداد کمی از حساب‌های رایانامه موافقت می‌کند.

این ابزار برای جست‌وجو در یک مجموعه‌ی مشخص از رشته‌های نویسه‌ی موجود در رایانامه‌های یاهو، و ذخیره‌ی آن‌ها برای بازیابی از راه دور طراحی شده بود، اما هنوز مشخص نیست که جاسوسان دقیقاً دنبال چه چیزی بوده‌اند.

در سال ۲۰۱۴ نیز با یک سند دادگاهی مواجه شدیم که نشان می‌داد یاهو، که مخالف تدابیر NSA بود، در سال ۲۰۰۸ حاضر نشده به برنامه‌ی نظارتی PRISM ملحق شود، یاهو تا زمانی روی تصمیم خود پافشاری می‌کرد که دولت آمریکا حرفی از جریمه‌ی ۲۵۰هزار دلاری در هر روز را به میان نیاورده بود.

اما آژانس اطلاعاتی آمریکا بار دیگر در سال ۲۰۱۵ با یک حکم دادگاه به این شرکت نزدیک شد؛ این حکم در قالب یک «دستور طبقه‌بندی‌شده» بود که به تیم حقوقی یاهو فرستاده شد.

تیم امنیتی یاهو، بی‌اطلاع از اوضاع

این ابزار جست‌وجوی رایانامه به‌طوری مرموز بود که حتی تیم امنیتی یاهو هم از برنامه خبری نداشت.

مدیر اجرایی یاهو، ماریسا مایر، و مشاور عمومی این شرکت، ران بل، نه‌تنها تصمیم گرفتند که خود را با این موضوع وفق دهند و با آژانس امنیت ملی آمریکا سر جنگ نداشته باشند، بلکه حتی تیم امنیتی یاهو را هم درگیر این ماجرا نکردند.

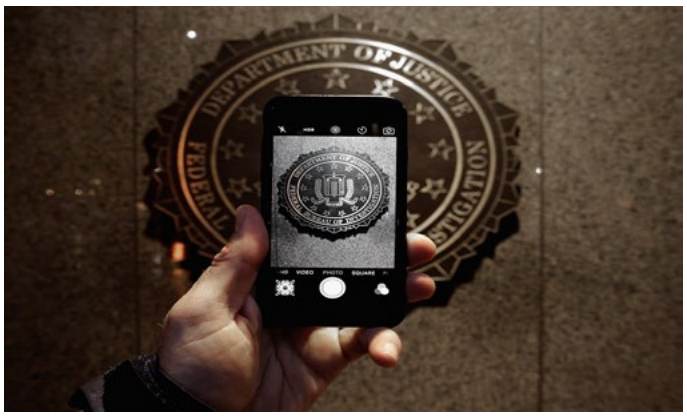
در عوض، مایر و بل از مهندسان رایانامه‌ی یاهو درخواست کردند تا یک برنامه‌ی نرم‌افزاری سری را برای آن‌ها ایجاد

کنند که این برنامه پیام‌های حاوی یک سری نویسه‌ی خاص را پیدا کند، برنامه‌ای که به نفع جاسوسان بوده و نویسه‌ها را برای بازیابی از راه دور ذخیره می‌کند.
بنابراین، هنگامی‌که تیم امنیتی یاهو این برنامه را در سال ۲۰۱۵ کشف کرد، در وهله‌ی اول تصور کرد که دسته‌ای از نفوذگران سعی داشته‌اند به یاهو نفوذ کنند.

افسر ارشد امنیت اطلاعات یاهو با نارضایتی این شرکت را ترک می‌کند
الکس استاموس، افسر ارشد امنیت اطلاعات یاهو، دریافت که مایر این برنامه‌ی نظارتی را تأیید کرده است؛ به همین خاطر از سمت خود در یاهو استعفا داد و به زیردستان خود گفت که از کاری که امنیت کاربران را به خطر بیاندازد، کناره‌گیری می‌کند.
استاموس در حال حاضر برای فیس‌بوک کار می‌کند.
یاهو در بیانیه‌ای کوتاه خطاب به رویترز گفت: «یاهو یک شرکت مطیع قانون است، و تابع قوانین ایالات متحده می‌باشد.»
این شرکت حاضر نشد بیشتر درباره‌ی این مقوله اظهار نظر کند.
این احتمال وجود دارد که شرکت‌های اینترنتی دیگر هم یک حکم دادگاهی مشابه را دریافت کنند، زیرا این آژانس جاسوسی، یعنی NSA، نمی‌داند که اهدافش از کدامین سرویس رایانامه استفاده می‌کنند.
از آن‌جایی‌که آژانس امنیت ملی آمریکا معمولاً درخواست‌های نظارتی خود را از طریق FBI ارائه می‌کند، پی بردن به این مسأله که کدام نهاد به دنبال اطلاعات است کمی سخت می‌شود.
این خبر کمی بعد از آن منتشر شد که یاهو اعلام کرد که قربانی یک حمله‌ی سایبری تحت حمایت دولت شده و اطلاعات شخصی بیش از ۵۰۰ میلیون کاربر آن به بیرون درز کرده است.

امنیت‌سایبری

FBI خواستار باز کردن قفل آیفون یک داعشی دیگر



افی‌بی‌آی در صدد آن است تا قفل آیفون یکی دیگر از تروریست‌های به هلاکت رسیده را باز کند.

ماه گذشته ضاهر عدن، که روی ۱۰ نفر در خیابان کلود مینه‌سوتا چاقو کشید، بعد از آن به ضرب گلوله‌ی یک افسر وظیفه‌ی پلیس کشته شد. پس از این ماجرا داعش مسئولیت حمله را بر عهده گرفت.

عدن، همانند یکی از عوامل حمله‌ی مسلحانه و تروریستی به نام رضوان فاروق، یک آیفون قفل‌شده داشت؛ در یک کنفرانس مطبوعاتی که در مینه‌سوتا برگزار شد، مأمور ویژه‌ی FBI، ریچ تورتون تأیید کرد که این آیفون را در اختیار گرفته و قصد دارد به محتوای آن دسترسی پیدا کند؛ تورتون هیچ اشاره‌ای به مدل این آیفون نکرد، بنابراین حدس این‌که سامانه‌ی عامل اپل این گوشی از چه نوعی است کمی سخت می‌شود.

تورتون گفت: «آیفون ضاهر عدن قفل است؛ ما در حال ارزیابی اختیارات قانونی و فنی خود برای دستیابی به محتوای این دستگاه و داده‌های احتمالی آن هستیم.»

از زمان انتشار iOS 8 در ۲۰۱۴، آیفون و آیپد با یک رمزگاری توکار ارائه شدند که کلیدهای مخفی آن‌ها در دسترس اپل نمی‌باشد. دسترسی به این کلید فقط و فقط برای مالک آن که از پین‌کد آن مطلع است، امکان‌پذیر می‌باشد.

در ابتدای سال ۲۰۱۶میلادی، یک منازعه‌ی حقوقی طولانی میان FBI و اپل درگرفت، در حقیقت FBI از اپل درخواست کرده بود تا یک کد سفارشی را بنویسد که امکان دسترسی به شیوه‌ی جست‌وجوی فراگیر را به آیفون 5c فاروق فراهم نماید. این کد به پلیس آمریکا اجازه می‌داد تا دیگر ۱۰ تلاش ناموفق برای باز کردن قفل گوشی فاروق نداشته باشد.

اپل با این خواسته‌ی دولت آمریکا مبنی بر ارائه‌ی یک راه حل قراردادی در دادگاه و ملاء عام مخالفت کرد، و این مخالفت تا زمانی ادامه پیدا کرد که FBI حاضر شد مبلغ ۱ میلیون دلار را برای نفوذ فنی به این گوشی و حل و فصل بن‌بست پیش‌آمده پرداخت کند. تحقیقات بعدی نشان داد که چگونه می‌توان حافظه‌ی فلش یک آیفون 5c را پیش از غیرفعال‌سازی شمارنده‌ی پین‌کدهای واردشده پاک کرد؛ پین‌کدهایی که به منظور حملات جست‌وجوی فراگیر وارد می‌شوند.

هزینه‌ی این روی‌کرد، که با هزینه‌ی پرداخت‌شده توسط مقامات فدرال آمریکا برای باز کردن قفل گوشی فاروق قابل مقایسه نیست، فقط روی گوشی آیفون 5c عمل می‌کند و به درد آیفون‌های جدید نمی‌خورد. ظاهراً در مدل‌های جدید آیفون کلیدهای رمزگذاری در یک سخت‌افزار امن‌تر و مقاوم‌تر ذخیره می‌شوند، سخت‌افزاری که حتی رشوه‌های کلان هم نمی‌توانند آن را رمزگشایی کند!

گویا عدن برای خرید یک آیفون ۷ به آن فروشگاه رفته است.

امنیت‌سایبری

ترکیه کشوری که بیشترین آلودگی به بات‌ها را دارد!

محققـان بخـش نورتـون در شرکـت Symantec می‌گوینـد ترکیـه بیش‌تریـن آلودگـی باتهـا را داراسـت به‌طوری‌کـه در ایـن کشـور بـه ازای هـر ۱۱۳۹ کاربـر اینترنتـی یـک بـات مشـغول بـه فعالیـت اسـت. در همیـن گـزارش آمـده اسـت کـه ترکیـه ۱۸.۵ درصـد از کل باتهـای موجـود در اروپـا، آسـیای میانـه و افریقـا را داراسـت.

نقشـه پراکندگـی بـات Symantec نشـان می‌دهـد کـه بیش‌تریـن رایانه‌هـای آلـوده شـده در دو شـهر اسـتانبول و آنـکارا واقـع شـده‌اند. ایـن دو شـهر باهـم نیمـی از جمعیـت ترکیـه را تشـکیل می‌دهنـد.

پـس از ترکیـه نیـز کشـورهای ایتالیـا، مجارسـتان، آلمان، فرانسـه، اسـپانیا، بریتانیـا، لهسـتان، روسـیه و رژیـم صهیونیسـتی بـه لحـاظ تعـداد باتهـا مقام‌هـای بعـدی را دارنـد.

نیـک شـاو، مدیـر بخـش EMEA در Symantec می‌گویـد: «تعـداد باتهـا بـه عوامـل مختلفـی بسـتگی دارد، امـا بازارهـا و شـهرهایی کـه اخیـراً بـه سـمت اسـتفاده از دسـتگاه‌های متصـل بـه اینترنـت متمایـل شـده‌اند، به‌طـور قطـع هدفـی جـذاب بـرای مجرمـان سـایبری بـه شـما می‌آینـد. بخـش دوم ایـن جورچیـن دسـتگاه‌هایی هسـتند کـه امنیـت کافـی نداشـته و به‌راحتـی توسـط ایـن مجرمـان مـورد نفـوذ واقـع می‌شـوند.»

اگـر کشـورهای مذکـور را برحسـب چگالـی بـات مرتـب کنیـم، مجارسـتان مقـام اول را خواهـد داشـت. در ایـن کشـور بـه ازای هـر ۳۹۳ کاربـر اینترنتـی یـک بـات وجـود دارد. مقام‌هـای بعـدی از آن کشـورهای موناکـو، آنـدورا، رژیـم صهیونیسـتی، ترکیـه، لاتویـا، کویـت، ایتالیـا، مـصر و لهسـتان اسـت.

پـاول وود، مدیـر بخـش امنیـت سـایبری در Symantc می‌گویـد: «مهـم اسـت کـه بـه ایـن نکتـه توجـه کنیـم، جایـی کـه باتهـا وجـود دارنـد لزومـاً بـه ایـن معنـا نیسـت کـه مجرمـان سـایبری کنترل‌کننـده ایـن باتهـا هـم در آنجـا زندگـی می‌کننـد. باتهـا به‌طـور طبیعـی موجودیتـی جهانـی هسـتند. یـک دسـتگاه آلـوده در اروپـا کـه توسـط مجرمانـی در آمریـکای شـمالی آلـوده شـده اسـت می‌توانـد در حملـه‌ای در آسـیا مشـارکت داشـته باشـد.»

امنیت‌سایبری

دستگیری مظنون اصلی سرقت ابزارهای نفوذ سازمان NSA

سازمان FBI می‌گوید یک پیمانکار دولتی را به اتهام سرقت اسناد محرمانه‌ای که شامل ابزارهای نفوذ نیز بوده، دستگیر کرده است.

به گفته وزارت دادگستری آمریکا، هارولد توماس مارتین ۵۱ ساله متهم شده است اسناد دولتی شامل اطلاعات فوق‌محرمانه را به سرقت برده است. وی که مسئول یک سازمان اطلاعاتی محرمانه بوده، متهم شده در سال ۲۰۱۴ شش مورد از اسناد سرّی را دزدیده است. وزارت دادگستری در این خصوص گفته است: «این اسناد از طریق منابع دولتی، روش‌ها و توانایی‌های حساس امنیتی ایجاد شده بودند و در بخش‌های مختلف امنیت ملی کاربرد داشته‌اند.» به گفته نیویورک تایمز، مارتین که یک پیمانکار سازمان NSA است به دلیل انتشار کد رایانه‌ای محرمانه‌ای دستگیر شده است که برای نفوذ به دولت‌های خارجی استفاده می‌شده است. او برای Booz Allen Hamilton کار می‌کرده است؛ همان بخشی که ادوارد اسنودن نیز در آن مشغول به کار بوده است. Booz Allen Hamilton که کار نگهداری زیرساخت‌های NSA را بر عهده دارد هنوز درباره مارتین اظهارنظری نکرده است.

مارتین یک هفته پس از آن دستگیر می‌شود که نفوذگران ناشناسی با عنوان ShadowBrokers به‌صورت برخط اقدام به انتشار ابزارهای نفوذ سازمان NSA کردند.

به گزارش وزارت دادگستری آمریکا، مارتین در بازجویی‌های اولیه سرقت هرگونه اسناد و ابزار محرمانه را رد کرده بود، اما بعداً این امر را تائید کرده و گفته می‌دانسته اجازه دسترسی به این اسناد را نداشته است. وکیل مارتین می‌گوید هنوز شواهد قابل استنادی که خیانت او را به کشور اثبات کند وجود ندارد.

اسناد دیجیتالی و چاپ‌شده‌ای از مدارک به سرقت‌رفته در خانه و خودرو مارتین در مریلند کشف و ضبط شده‌اند. اگر جرم مارتین اثبات شود وی احتمالاً باید به خاطر سرقت اسناد دولتی و دسترسی غیرمجاز به ابزارهای محرمانه ۱۱ سال زندان را متحمل شود. سازمان NSA هنوز درباره این خبر اظهار نظری نکرده است.

امنیت‌سایبری

چانه‌زنی یک میلیارد دلاری شرکت Verizon برای خرید یاهو پس از رسوایی امنیتی

به نظر می‌رسد اخبار بد برای یاهو تمامی ندارد. این بار منبع خبر برای این شرکت، Verizonاست. این شرکت که پیش از این قبول کرده بود یاهو را به قیمت 8/4 میلیارد دلار بخرد، حالا می‌گوید به خاطر گزارش‌های اخیر درباره رخنه‌های امنیتی رخ داده در یاهو قیمت خود را یک میلیارد دلار کم کرده است.

تنها دو هفته پیش یاهو فاش کرد که حداقل نیم میلیارد حساب کاربری این شرکت در نفوذ سال ۲۰۱۴ به سرقت رفته‌اند تا بدین ترتیب از بزرگ‌ترین رخنه داده‌ای تاریخ پرده برداشته شود. این هفته نیز شرکت یاهو با اتهاماتی مواجه شد مبنی بر این‌که این شرکت سال گذشته به دستور آژانس اطلاعاتی آمریکا با ساخت یک ابزار سری همه رایانامه‌های کاربران خود را پویش می‌کرده است.

نیویورک‌تایمز می‌گوید تیم آرمسترانگ، مدیرعامل AOL که از شرکت‌های تابعه Verizon محسوب می‌شود درباره انفاقات اخیر اظهار تأسف کرده و احتمال داده است که قرارداد بین یاهو و Verizon باقیمت پایین‌تری انجام شود. آرمسترانگ می‌گوید درباره قیمت پایین‌تر با مقامات یاهو در حال گفتگو است اما یاهو از سوی دیگر گفته معامله انجام شده است و به لحاظ قانونی نمی‌توان آن را تغییر داد.

Veriozn در ماه جولای اعلام کرد با یاهو به توافق رسیده است تا با خرید این شرکت آن را با AOL تلفیق کند. Veriozn می‌گوید با این کار می‌خواهد رقابت خود را با شرکت‌هایی همچون گوگل و فیسبوک برای تبلیغات دیجیتال جدی‌تر کند. گفته می‌شود تملک یاهو احتمالاً اوایل سال آینده میلادی انجام می‌شود تا خدمات تبلیغ، تلفن‌همراه و جستجوی یاهو با AOL تلفیق شده و بدین ترتیب کاربران آن‌ها به یک میلیارد نفر برسد.

امنیت‌سایبری

از این پس وزرای بریتانیا نمی‌توانند ساعت اپل را هم در جلسات کابینه دولت همراه خود داشته باشند

خرابکاری‌های امنیتی اخیر، رشته حملات سایبری علیه انتخابات ریاست جمهوری آمریکا و فشار نفوذگرهای چینی اخیراً موجب جلب‌توجه افراد زیادی به حوزه امنیت سایبری شده است. در سال ۲۰۱۳ وزرای کابینه بریتانیا از آوردن گوشی‌های هوشمند و همچنین تبلت به جلسات هیئت وزیران منع شدند. در همین راستا و به دلیل واهمه از استراق سمع توسط عوامل خارجی، دولت بریتانیا تصمیم گرفت اعضای کابینه را از داشتن آی‌پد نیز محروم کند.

خبرهای منتشر شده از سوی Mailحاکی از آن است که در جریان سخنرانی وزیر دفتر کابینه، فرانسیس ماد، وی از آی‌پد خود برای ارائه مطالب استفاده کرده است اما کارمندان امنیتی دفتر نخست‌وزیری دستگاه وی را گرفته‌اند تا از استراق سمع احتمالی پیشگیری کرده باشند.

اما حالا وزرای کابینه از به همراه آوردن ساعت اپل در جلسات داخلی نیز منع شده‌اند تا یک راه دیگر برای استراق سمع این جلسات محدود شده باشد. دولت بریتانیا معتقد است نفوذگرهای روسی توانسته‌اند این دسته از دستگاه‌ها را مورد نفوذ قرار داده و به اطلاعات حساس دست یابند.

به نظر می‌رسد در زمان نخست‌وزیری دیوید کامرون ساعت‌های اپل در بین وزرای کابینه طرفداران زیادی داشته است، اما حالا باوجود نخست‌وزیری ترزا می، شرایط تغییر کرده است و چنین دستگاه‌هایی که امکان استراق سمع را برای دولت‌های خارجی ممکن می‌ساخته‌اند بیش‌تر منع شده‌اند. به گفته متخصصان، این تصمیم درباره دستگاه‌های پوشیدنی گرفته شده است تا خدمات امنیتی دولت‌های خارجی راه سخت‌تری برای دست‌یابی به اطلاعات حساس داشته باشند.

امنیت‌سایبری

اجازه‌ی هک پیام‌رسان فیس‌بوک، اسکایپ و واتس‌اپ توسط قانون ضدتروریسم روسیه

قانونی که اخیراً در روسیه به تصویب رسیده است به شرکت‌های امنیتی این اجازه را می‌دهد تا ارتباطات رمزنگاری‌شده‌ی پیام‌رسان فیسبوک، اسکایپ و واتس‌اپ را هک کنند.

قانون Yarovaya به عنوان یک اقدام ضدتروریستی به تصویب رسیده است. کارمندی که با شرکت امنیتی Con Certeza همکاری می‌کند و مسئول توسعه‌ی ابزارهایی برای اعمال قانون است، اخیراً به انتشارات Kommersant روسیه گفت که شرکت آن‌ها در حال تحقیق برای دسترسی به اطلاعات حساسی برای شناسایی احزاب، به دست آوردن اعتبارنامه‌های آن‌ها و انجام حمله‌ی مرد میانی علیه آن‌ها است.

Letallknow گفته‌های این کارمند را گزارش می‌دهد: «ما قصد داریم تا پیام‌رسان‌های اصلی همچون واتس‌اپ، وایبر، پیام‌رسان فیس‌بوک، تلگرام و اسکایپ برای iOS و اندروید را بررسی کنیم.»

این قانون نیازمند این است تا شرکت‌های ارتباطی و حوزه‌ی رسانه‌های اجتماعی کلیدهای رمزنگاری را بدست آورند و به سازمان‌های امنیتی دولتی کمک کنند. این قانون همچنین شرکت‌های ارتباطی را ملزم می‌کند تا داده‌ها و ترافیک بر روی کارگزارهای خود را برای مدت 3 سال نگهداری کنند که این بازه‌ی زمانی برای شرکت‌های رسانه‌ی اجتماعی یک سال در نظر گرفته شده است.

امنیت‌سایبری

ترکیه برای سانسور کردن افشاگری گروه RedHack سرویس‌های گیت‌هاب، دراپ‌باکس و گوگل درایو را مسدود کرد.

ترکیه مجدداً با تحریم کردن سرویس‌های برخط در صدر خبرها قرار گرفته است و این در حالی است که این سرویس‌ها مربوط به غول‌های بزرگ تکنولوژی است.

بنا به گزارش‌ها دولت ترکیه دسترسی به سرویس‌های اَبری برخط همچون مایکروسافت OneDrive، دراپ‌باکس، گوگل درایو و همچنین سرویس میزبانی کد گیت‌هاب را مسدود کرد.

این سرویس‌ها روز یک‌شنبه در پی افشای رایانامه‌های وزیر انرژی و منابع طبیعی Berat Albayrak و همچنین پسر قانونی رئیس جمهور رجب طیّب اردوغان، مسدود شده است.

گیت‌هاب، دراپ‌باکس و گوگل درایو دارای خطاهای SSL بودند که رهگیری ترافیک در سطح ملی و یا ISP ها را ممکن می‌ساخت. مایکروسافت OneDrive نیز در این قضیه مسدود شده است.

این افشاگری توسط یک گروه نفوذ 20 ساله با نام RedHack انجام شده است که حاوی 17 گیگابایت پرونده مربوط به 57623 رایانامه به سرقت رفته است که قدمت آن به آوریل سال 2000 تا سپتامبر همین امسال می‌رسد.

دادگاهی در ترکیه صحت این داده‌های افشاء شده را تائید کرد.

این حرکت مسدود کردن سرویس‌های مذکور به نظر می‌رسد برای سرکوب کردن چرخش رایانامه‌های به سرقت‌رفته و جلوگیری از میزبانی این رایانامه‌ها توسط کاربران بر روی حساب‌های خود باشد که ممکن است یک پویش تبلیغاتی و فریبنده را راه بیندازد.

بنا به گزارش Turkey Blocks سرویس گوگل درایو روز یک‌شنبه از مسدود بودن خارج شد ولی سایر سرویس‌ها همچنان در داخل کشور غیرقابل دسترس هستند.

ترکیه نیز شبیه به چین، از خیلی وقت پیش به این عنوان شناخته شده که سرویس‌های برخط را مسدود می‌کند تا کاربران اینترنتی از آنچه که دولتمردان انجام می‌دهند باخبر نشوند. در ماه مارس نیز در پی انفجار یک ماشین بمب‌گذاری‌شده در آنکارا، این کشور استفاده از شبکه‌های اجتماعی فیس‌بوک و توییتر را ممنوع کرد.

ماجرایی شبیه به در ماه مارس سال 2014 نیز اتفاق افتاد. زمانی که توییتر در ترکیه تحریم شد و دلیل آن یک کلیپ ویدئویی منتشرشده در توییتر و یوتیوب در مورد فساد گسترده رئیس جمهور رجب طیب اردوغان بود که به پسرش آموزش می‌دهد تا ترتیب مقدار زیادی پول را در میان بررسی‌های پلیس بدهد.

و همچنین این اولین‌باری نیست که نفوذگران اطلاعات شخصی اعضای مهم دولت را فاش می‌کنند. چند ماه قبل، اطلاعات شخصی تقریباً 50 میلیون شهروند ترکیه‌ای از جمله رئیس جمهور رجب طیّب اردوغان به‌طور برخط منتشر شد.

امنیت‌سایبری

آمریکا رسماً دولت روسیه را در هک‌های مربوط به انتخابات مقصر می‌داند!

مقامات ایالات متحده رسماً دولت روسیه برای چند هک سطح بالا علیه گروه‌های سیاسی سرزنش می‌کند و ادعا می‌کنند که این عملیات به معنای تداخل در انتخابات آینده است.

وزارت امنیت داخلی و دفتر مدیر اطلاعات ملی در بیانیه‌ای خبر داد که سازمان‌های اطلاعاتی ایالات متحده، با اطمینان روسیه را مسئول می‌دانند.

آن‌ها ادعا می‌کنند که دولت روسیه رایانامه مقامات و نهادهای ایالات متحده را به خطر انداخته و سپس آن‌ها به‌طور برخط و عمومی در وب‌گاه‌های WikiLeaks، DCLeaks و توسط هکر گمنام Guccifer 2.0 منتشر کرده است که با توجه به این مسائل نقض اعتبار کمیته ملی حزب دموکرات در اوایل سال جاری صورت گرفت.

در این بیانیه آمده: «این دزدی و افشاء برای مداخله در فرایند انتخابات ایالات متحده، صورت گرفته است.»

اگر چه سازمان‌ها شواهد خاصی برای این ادعا ندارند، آن‌ها گفتند: «روش‌ها و انگیزه‌های پشت هک سازگار با تلاش‌هایی با کارگردانی روسیه است.»

در این بیانیه آمده است: «چنین فعالیت‌هایی از سمت مسکو، فعالیت جدیدی نیست. روس‌ها تاکتیک‌های مشابهی در سراسر اروپا و اوراسیا استفاده کرده‌اند به عنوان مثال برای نفوذ به افکار عمومی»

این سازمان‌ها همچنین عنوان کردند افسران ارشد روسیه می‌توانند مجوز چنین حمله‌ای را صادر کرده باشند. سفارت روسیه بلافاصله به این درخواست پاسخ نداد. اما دولت این کشور، بارها و بارها هرگونه دخالت در این هک‌ها را تکذیب کرد.

شاید جدی‌ترین هک، نقض در کمیته ملی حزب دموکرات باشد. در ماه ژوئن، گزارش داده شد که هکرها پرونده‌های حساس همچون پژوهش مخالفان علیه نامزد ریاست جمهوری، دونالد ترامپ از این گروه را به سرقت برده‌اند. یک هکر که خود را Guccifer 2.0 نامیده، در ویکی‌لیکس این پرونده‌ها را به‌طور برخط پست کرده است.

در یکی دیگر از هک‌های جدی در ماه سپتامبر، رایانامه به سرقت‌رفته از وزیر سابق امور خارجه کالین پاول به‌طور برخط از طریق یک وب‌گاه به نام DCLeaks منتشر شده است.

کارشناسان امنیتی مشکوک هستند که همه این حوادث ممکن است بخشی از یک پویش تحت حمایت روسیه، برای شکل دادن به پوشش رسانه‌ای انتخابات در ایالات متحده باشد و به شانس نامزد دموکرات، هیلاری کلینتون برای ریاست جمهوری در انتخابات آسیب برساند.

مقامات اطلاعاتی ایالات متحده به‌طور خصوصی معتقد هستند که روسیه در برخی از این حوادث دخالت دارد، اما به‌طور رسمی هیچ چیز تا جمعه گفته نشد.

سازمان‌های اطلاعاتی همچنین گفتند برخی از کشورهای ایالات متحده به تازگی تجربه «پویش و کاوش» سامانه‌های

مربوط به انتخابات را داشتند که این کارگزار توسط یک شرکت روسی اداره می‌شود.

بیانیه‌ی روز جمعه اشاره می‌کند: «با این حال، ما در حال حاضر در موقعیتی نیستیم که این فعالیت‌ها را به دولت روسیه نسبت دهیم.»

وزارت امنیت داخلی، مصرانه مسئولان انتخابات ایالتی و محلی را به هوشیاری و کمک به امنیت سایبری دعوت می‌کند. این عملیات در چندین ایالت در حال حاضر انجام می‌شود. اما این سازمان همچنین گفت که هک کردن سامانه‌ی انتخابات ایالات متحده دشوار خواهد بود با توجه به اینکه این سامانه‌ها در سراسر 50 ایالت توزیع شده‌اند و در حال حاضر حفاظت می‌شوند.

امنیت‌سایبری

پویش OilRig دولت آمریکا و شبکه‌های انرژی را هدف قرار داده است

پویش OilRig یک گروه نفوذ ایرانی که قبلاً سازمان‌های عربستان سعودی را هدف قرار داده بود، اینک سایه‌ی خود را بر سایر کشورها نیز انداخته است.

نفوذگران ایرانی که قبلاً سازمان‌های عربستان سعودی را هدف قرار داده بودند هم‌اکنون سازمان‌های سایر کشورها از جمله آمریکا را تحت عنوان کمپین OilRig هدف قرار داده‌اند.

علاوه بر گسترش دستاوردها، این گروه ابزار بدافزاری خود را نیز بهبود داده است. محققان در بخش شبکه‌ی Palo Alto این گروه را برای مدتی تحت نظر قرار دادند و مشاهده کردند که عملیات این گروه علیه سازمان‌های مالی و تکنولوژی عربستان و همچنین علیه صنعت دفاعی آن انجام شده است. این پویش تحت عنوان OilRig شامل صفحات گسترده‌ی اکسل مایکروسافت ردیابی شده با عنوان Clayslide و یک درب ِ پشتی با نام Helminth است.

حملات بانکی توسط گروه ایرانی، توسط FireEye در ماه می تحلیل و مستند شده است. Palo Alto گزارش داده که این کمپین سازمان‌هایی در قطر و برخی سازمان‌های حکومتی آمریکا، رژیم صهیونیستی و ترکیه را نیز هدف قرار داده است.

درب ِ پشتی Helminth توسط عاملان این تهدید از طریق رایانامه‌های فیشینگ نیزه‌ای و اسناد مخرب اکسل که قابلیت ماکرو در آن‌ها فعال شده، تحویل داده می‌شود. برای نمونه، در مورد سازمان‌های حکومتی ترکیه، پرونده‌ی اکسل طوری طراحی شده تا پورتال خطوط هوایی را ارائه دهد.

4 نوع از بدافزار Helminth وجود دارد که قادر هستند از طریق پروتکل HTTP و DNS با کارگزار دستور و کنترل خود ارتباط برقرار کنند و همچنین اطلاعات حساس و مهم را از دستگاه آلوده‌شده بدست آورده و پرونده‌های اضافی را از طریق کارگزار راه دور بارگیری کنند. یکی از نمونه‌های بدافزار Helminth مبتنی بر اسکریپت PowerShell و VBScript است. یکی دیگر از نسخه‌ها در قالب یک پرونده‌ی اجرایی توسعه داده شده است. این نسخه توسط یک تروجان با نام مستعار HerHer تحویل داده شده و قابلیت ثبت کلیدهای فشرده‌شده در دستگاه قربانی را دارد.

در گزارش منتشرشده توسط PaloAlto آمده: «آرشیو Zip با یک گذرواژه‌ی ناشناس رمزنگاری شده است ولی ما می‌دانیم که حاوی دو پرونده با نام‌های joboffer.chm و thumb.db است. پرونده‌ی thumb.db نام و اندازه‌ای برابر با قراردهنده‌ی تروجانی دارد که ما آن را با عنوان HerHer ردیابی کردیم که یک نمونه‌ی اجرایی از بدافزار Helminth را نصب می‌کند.»

با توجه به منشأ عاملان این تهدید، محققان سرنخ‌های مختلفی را کنار هم قرار داده و متوجه شدند که عاملان

اشخاصی ایرانی هستند. هرچند آن‌ها معتقدند که می‌توان داده‌ها را به راحتی جعل کرد. گروه Palo Alto که فعالیت چندین گروه نفوذ را زیر نظر دارد، معتقد است این عملیات از ایران ناشی می‌شود. یکی از این گروه‌ها از بدافزاری بهره می‌برد که Infy نامیده می‌شود. در طول تابستان این شرکت امنیتی گزارش داده است که یک کمپین جاسوسی سایبری تحت عنوان Infy را مختل کرده است.

همچنین در ماه آگوست متوجه شد که نفوذگران ایرانی پیام‌رسان تلگرام را آلوده کرده‌اند، که به آن‌ها اجازه‌ی دسترسی به اطلاعات حساب‌های 15 میلیون کاربر ایرانی را می‌دهد. حساب‌های نقض شده بیشتر مربوط به روزنامه‌نگاران و اشخاص مهم ایرانی بوده است. این حمله فعال‌سازی یک‌باره‌ی پیامکی تلگرام را هدف قرار داده بود و ربطی به رمزنگاری انتها به انتها در تلگرام نداشت.

تلگرام زمانی که کاربر می‌خواهد از یک دستگاه جدید وارد حساب خود شود، یک پیامک اعتبارسنجی را ارسال می‌کند. اما این پیامک می‌تواند توسط شرکت‌های تلفن شنود شده و به نفوذگران فروخته شود که در نتیجه مهاجمان می‌توانند به لیست مخاطبان و گفتگوهای کاربران دسترسی یابند.

و در اواخر سال، نگرانی از این نفوذگران مخرب درخصوص هدف قرار دادن بخش انرژی وجود دارد. براساس مطالب RegBlog:

«خطرات سایبری بیش از حد برای سازمان‌ها و شبکه‌های برق متصل به اینترنت وجود دارد. با توجه به گزارش امنیت داخلی از وزارت ایالات متحده، اگر چه بخش انرژی تنها 5 الی 6 درصد از تولید ناخالص داخلی ایالات متحده را تشکیل می‌دهد، اما در 32 درصد از موارد این صنعت، هدف حملات سایبری بوده است.

حوادث اخیر آسیب‌پذیری در سامانه تامین برق را پررنگ‌تر و راه را برای لایحه‌ای برای اقدامات سایبری هموارتر کرده است. یک رخداد مربوط به ماه مارس زمانی که گروهی از نفوذگران ایرانی برای چندمین با یک سد کوچک در جنوب نیویورک را در سال 2013 هدف قرار داده بودند، است. همچنین بسیاری از شرکت‌های مالی را هدف قرار داده بودند و بر سطح آب این سد دسترسی و کنترل داشتند. این موضوع آسیب کمی داشت در کنار زحمت و دردسری که برای مشتریان به‌وجود آمد ولی همچنان یک تهدید بالقوه به شمار می‌رود.»

بنابراین عاملان تهدید ایرانی به تدریج از تهدید و حملات بانکی به سمت هدف قرار دادن شبکه‌های انرژی حرکت می‌کنند. در ضمن این واقعیت که نفوذگران قادر به در دست گرفتن کنترل سامانه‌های اساسی ما باشند، بسیار نگران‌کننده است. نفوذ به شبکه‌ها و مخصوصاً شبکه‌های انرژی پتانسیل تأثیری شدید و گسترده دارد.

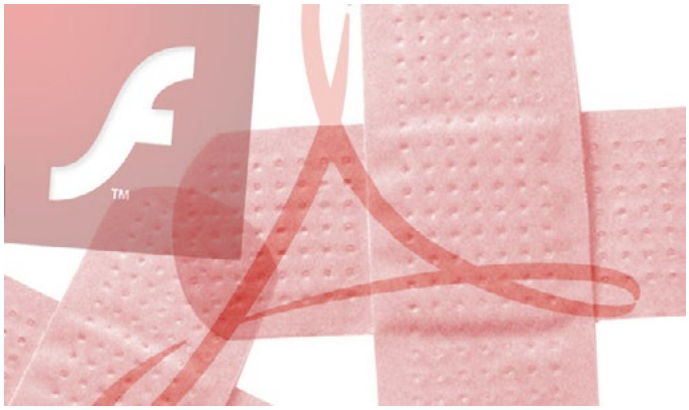
پی‌نوشت: فعالیت‌های این گروه از نفوذگران، از نظر ما تایید شده نیست و شاید این گزارش‌ها بخشی از برنامه‌ی دولت‌های متخاصم برای وارونه جلوه دادن ماجرا باشد، تا به اشتباه سایر کشورها را از قدرت سایبری ایران ترسانده و سپس عملیات مقابله با آن را آغاز کنند.

فصل چهارم

اخبار فنی

اخبار فنی

ادوبی ۸۱ آسیب‌پذیری آکروبات، فلش و ریدر را رفع کرد



ادوبی ۸۱ آسیب‌پذیری موجود در آکروبات ریدر و فلش را وصله کرده است؛ این آسیب‌پذیری‌ها شامل تعداد انگشت‌شماری از اشکالات مهم هستند که در صورتی که از آن‌ها سوءاستفاده شود، به نفوذگر اجازه می‌دهند تا کنترل یک سامانه را در اختیار بگیرد. ۷۱ مورد از کل آسیب‌پذیری‌های رفع‌شده متعلق به بسترهای آکروبات و ریدر بوده‌اند.

با نگاهی به بولتن امنیتی که توسط این شرکت مطرح در روز سه‌شنبه منتشر شده است، می‌توان گفت که بیشتر به‌روزرسانی‌های انجام‌شده برای آکروبات و ریدر منجر به اصلاح آسیب پذیری‌هایی همچون تخریب حافظه، استفاده بعد از آزادسازی، و سرریز بافر می‌شود که این موارد می‌توانند باعث اجرای کد در این نرم‌افزار شوند. دو وصله‌ی دیگر نیز منجر به رفع محدودیت اجرای رابط برنامه‌نویسی کاربردی جاواسکریپت و یک آسیب‌پذیری دور زدن امنیت می‌شوند که در این نرم‌افزار وجود دارد. این به‌روزرسانی Acrobat DC و Reader DC را به نسخه‌ی 15.006.30243 ارتقاء می‌دهد، همچنین باعث ارتقای Acrobat XI و Reader XI به نسخه‌ی 11.0.18 روی دستگاه‌های ویندوز و مکینتاش می‌شود.

این وصله‌ها نخستین مواردی هستند که از ماه جولای برای آکروبات و ریدر منتشر شده‌اند؛ در ماه جولای ادوبی ۳۸ مشکل موجود در این نرم‌افزار را اصلاح نمود. اصلاحیه‌ی این ماه شامل بیشترین تعداد به‌روزرسانی است که از ماه می امسال برای این نرم‌افزار ارائه شده است، در ماه می این شرکت ۹۳ آسیب‌پذیری آکروبات و ریدر را رفع نمود.

۱۲ آسیب‌پذیری وجود دارد که فلش‌پلیر موجود در کروم، مایکروسافت اج، نسخه‌ی ۱۱ اینترنت اسکپلورر، و لینوکس را تحت شعاع قرار داده است؛ این آسیب‌پذیری‌ها نیز امروز حل و فصل شدند. اکثر وصله‌ها نظیر خطاهای ریدر و آکروبات، که شامل ۹ مورد از ۱۲مورد هستند، از نوع تخریب حافظه می‌باشند. یکی از محققان شبکه‌ی پالو آلتو به نام تائو یان که ۸ آسیب‌پذیری را در ماه گذشته در فلش کشف کرده است، توانسته ۴ مورد از مجموع ۹ آسیب‌پذیری را پیدا کند که همگی از نوع تخریب حافظه بوده‌اند و ادوبی آن‌ها را در روز سه‌شنبه اصلاح نموده است.

یک آسیب‌پذیری دور زدن امنیت، یک نوع سردرگمی در نوع و یک آسیب‌پذیری استفاده بعد از آزادسازی وجود دارند که می‌توانند باعث اجرای کد شوند، این آسیب‌پذیری‌ها نیز در فلش رفع شده‌اند. این ۱۲ آسیب‌پذیری موجود در فلش از به‌روزرسانی ماه گذشته رو به کاهش گذاشته‌اند؛ ماه گذشته ادوبی ۲۹ مشکل را رفع کرد، که بیشتر آن‌ها باعث اجرای کد می‌شدند. همچنین ادوبی این فرصت را روز سه‌شنبه داشته تا برنامه‌ی رومیزی Creative Cloud خود را اصلاح نماید؛ این

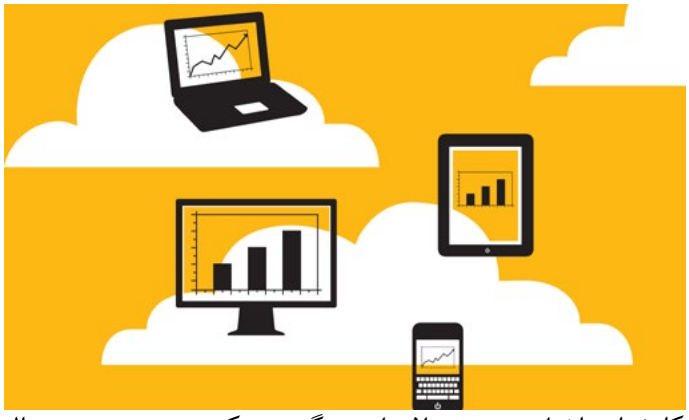
برنامه به کاربران ادوبی که عضو بستر Creative Cloud هستند اجازه می‌دهد تا برنامه‌ها و سرویس‌های خود را مدیریت نمایند. این به‌روزرسانی باعث برطرف شدن آسیب‌پذیری مسیر جست‌وجوی نقل‌قول شده در این برنامه می‌شود.

این آسیب‌پذیری به‌طور کلی از روشی که برنامه مسیرهای دایرکتوری را پارس (تجزیه) می‌کند برای اجرای کد استفاده می‌نماید. در این مورد، چنانچه از این آسیب‌پذیری سوءاستفاده شود، به منابع موجود در مسیر والد و مسیرهای پس از آن اجازه‌ی دسترسی داده می‌شود و این خود باعث بروز تشدید امتیاز می‌گردد.

ادوبی می‌گوید که تاکنون متوجه هیچ سوءاستفاده‌ای از این آسیب‌پذیری‌ها نشده است، اما این شرکت در قالب پستی که در وب‌لاگ پاسخ‌گویی به رخدادی رایانه‌ای خود منتشر کرد کاربران را تشویق به به‌روزرسانی به نسخه‌های جدید خود نمود.

اخبار فنی

اصلاح آسیب‌پذیری دور زدن احراز هویتِ SAP پس از ۳ سال!



کارشناسان امنیت نرم‌افزار می‌گویند که مدت سه سال است که یک آسیب‌پذیری حیاتی SAP وصله نشده است؛ هفته‌ی گذشته جزئیات این آسیب‌پذیری فاش شد.

به‌روزرسانی امنیتی ماهانه‌ی SAP روز سه‌شنبه منتشر شد؛ در این به‌روزرسانی به ۴۸ آسیب‌پذیری ترتیب اثر داده شد که در میان آن‌ها یک آسیب‌پذیری دور زدن احراز هویت نیز در سرویسی به نام P4 به چشم می‌خورد.

این سرویس یک کنترل از راه دور را به بستر جاوای SAP نظیر همه‌ی سامانه‌های پورتال SAP ارائه می‌کند. این آسیب‌پذیری دور زدن احراز هویت در P4 ساز و کاری را برای نفوذگران فراهم می‌آورد تا به واسطه‌ی آن بتوانند اطلاعات حساس را بخوانند.

سه سال پیش SAP سعی کرد این شکاف را از میان بردارد اما وصله‌ای که در نظر گرفت ناقص بود، و سامانه‌های بسیاری را آسیب‌پذیر رها کرد.

این مشکل برای اولین بار در سال ۲۰۱۲ گزارش و وصله شد. اما در یکی از آزمون‌های نفوذ کاشف به عمل آمد که این مشکل هنوز هم تقریباً تمامی نسخه‌های این سرویس را درگیر خود کرده است.

به عنوان مثال سرویس پک 0.9 برای نسخه‌ی 7.2 که آسیب‌پذیر است، در سال ۲۰۱۳ منتشر شده است.

سرویس آسیب‌پذیر P4 معمولاً در معرض اینترنت قرار دارد، عاملی که باعث می‌شود بهره‌برداری‌های احتمالی آسان‌تر شود.

پویش انجام‌شده توسط محققان نشان می‌دهد که دست کم ۲۵۶ سرویس آسیب‌پذیر وجود دارد که به‌طور برخط در دسترس هستند.

با نگاهی به سوابق SAP در ارائه‌ی وصله‌های اخیرش می‌توان گفت که SAP مشکلات امنیتی را با تأخیر وصله می‌کند. مثلاً این شرکت نرم‌افزاری فقط یک شکاف افشای اطلاعات نه چندان جدی را در ماه جولای وصله کرد؛ شکافی که مجدداً سه سال بعد بروز نمود. هیچ شواهدی وجود ندارد که نشان دهد یک کاربر مشکل حادی را در نتیجه‌ی این تأخیر لمس کرده است.

پایگاه خبری El Reg از SAP دعوت به عمل آورده تا در مورد انتقاد ضمنی از تأخیر این شرکت در تحویل وصله‌ی مناسب برای شکاف دور زدن احراز هویت نظر خود را اعلام نماید.

این شرکت امنیتی می‌گوید: «تیم پاسخ‌گویی به رخدادهای امنیتی محصولات SAP به‌طور مداوم با شرکت‌های تحقیقاتی مانند ERPScan هم‌کاری می‌کند تا از افشای مسئولانه‌ی آسیب‌پذیری‌ها مطمئن شود. وصله‌های امنیتی را می‌توان از فروشگاه سرویس‌های SAP بارگیری کرد.

به‌طور جدی به کاربران توصیه می‌شود تا چشم‌انداز SAP خود را با اعمال وصله‌های امنیتی موجود امن سازند، وصله‌هایی که در فروشگاه سرویس‌های SAP موجود هستند.

اخبار فنی

محققان از ماژول RKP برای نفوذ به Samsung KNOX استفاده کردند

محققان امنیتی شرکت Viral Security Group توانسته‌اند با سوءاستفاده از آسیب‌پذیری‌هایی که در دستگاه‌های وصله‌نشده‌ی در معرض خطر قرار دارند، قابلیت‌های امنیتی سامسونگ ناکس را دور بزنند.

این محققان برای عبور موفقیت‌آمیز از تدابیر امنیتی سامسونگ، روی ماژولی به نام TIMA RKP تمرکز کرده‌اند، که این ماژول مسئول دفاع برابر سوءاستفاده‌های احتمالی از هسته است. یک نفوذ به روت یا ریشه می‌تواند نظم هسته را به هم بریزد و کد مورد نظر نفوذگر را در سامانه‌ی کاربر به اجرا درآورد.

بنا به اظهارات مندرج در مقاله‌ی مربوط به این تحقیق، یک عامل مخرب با دسترسی به حساب کاربری سامانه می‌تواند برنامه‌های کاربردی مجاز را با نرم‌افزارهای مخربی جای‌گزین کند که به تمامی مجوزها دسترسی دارند و همه‌ی این مجوزها بدون اطلاع کاربر اعطا شده است. علاوه بر این، ماژول RKP می‌تواند برای دسترسی به امتیازهای ریشه مورد سوءاستفاده قرار گیرد، و پژوهش‌گران امنیتی حتی موفق شده‌اند یک ماژول کرنل یا هسته را در پارتیشن /system به عنوان یک ماژول قابل نوشتن بارگذاری نمایند.

پژوهش‌گران به منظور واژگون‌سازی ماژول RKP، از آسیب‌پذیری با شناسه‌ی CVE-2015-1805 به کمک بسته‌ی نفوذی متن‌باز iovyroot سوءاستفاده کرده‌اند. iovyroot که یک بسته‌ی نفوذ مبتنی بر لینوکس است برای سوءاستفاده از شکاف مورد بحث در دستگاه‌های نوظهور سامسونگ مانند گلکسی S6 و گلکسی نوت ۵ تدارک دیده شده است.

محققان می‌گویند که ماژول RKP دارای دو لایه است، یک لایه با هسته‌ی لینوکس در ارتباط است، و لایه‌ی دیگر به عنوان یک ناظر در ARM TrustZone جای گرفته است.

وظیفه‌ی RKP پوشش و حفاظت از نواحی خاصی از حافظه‌ی هسته است، تا بتواند بررسی‌ها و اعتبارسنجی‌های آن ناحیه‌ها را پنهانی و مستقل از هسته انجام دهد.

مشکل مطرح در مورد RKP تابع خاص rkp_override_creds است، که تابع override_creds متعلق به هسته را جای‌گزین می‌کند، می‌توان از این تابع برای لغو موقت اعتبار فرآیند کنونی استفاده کرد.

پژوهش‌گران با سوءاستفاده از این مشکل تلاش کرده‌اند تا با لغو اطلاعات محرمانه با اعتبارات روت توسط RKP به آن دست پیدا نمایند، اما ناموفق بوده‌اند؛ زیرا سمت ناظر برای لغو اطلاعات محرمانه‌ی فرآیند با اطلاعات روت تلاشی نمی‌کند. اما اعتبارات سامانه را می‌پذیرد.

محققان که هنوز مشغول تلاش برای رسیدن به ریشه هستند، پرونده‌ای به نام vmm.elf را پیدا کرده‌اند، که به نظر می‌رسد یک ماژول RKP باشد. آن‌ها توانسته‌اند در

این ماژول تابعی را بیابند که به آن‌ها اجازه می‌دهد به ریشه دسترسی داشته باشند.

اما محققان دریافته‌اند که مجوزهای موجود محدود است، و اجرای ماژول کرنل یا هسته منجر به تشدید امتیاز می‌شود، خصوصاً از وقتی که سامسونگ S6 امکان اضافه‌کردن ماژول‌های هسته را فراهم آورده است.

با این حال، این ماژول‌ها می‌بایست امضا شوند، و فرآیند تأیید آن‌ها بایست توسط میکرو کرنل Mobicore در TrustZone صورت گیرد.

با این وجود، از آن‌جایی‌که تأیید تنها زمانی انجام می‌شود که متغیر lkmauth_bootmode برای BOOTMODE_ RECOVERY تنظیم شود، پژوهش‌گران امنیتی از یک هسته برای درج آسیب‌پذیری برای بازنویسی مقدار متغیر و از کار انداختن سامانه‌ی تأیید امضا کمک گرفته‌اند.

در این مرحله محققان توانسته‌اند که به آسانی هر ماژول کرنلی را در نظر داشتند بارگذاری کنند. ۳ آسیب‌پذیری که امکان نفوذ موفق به سامسونگ ناکس را فراهم می‌کند، KNOXout نامیده می‌شوند. این آسیب‌پذیری‌ها که شناسه‌ی CVE-2016-6584 بدان‌ها تعلق گرفته، از نوع تشدید امتیاز هستند و در حال حاضر به فروشندگان محصولات درگیر با آن‌ها هشدارهای لازم داده شده است.

برخی از راه حل‌های پیشنهادی توسط محققان امنیتی شامل اصلاح مجوزهای سامانه‌ای مشابه ریشه است؛ در ادامه بررسی PID برای فرآیند اعطای مجوز انجام می‌شود، زیرا RKP به فرآیندهایی با PID برابر صفر امتیازهای ریشه را اعطا می‌کند (که محققان از همین نکته استفاده کرده‌اند)؛ و قرار دادن متغیر lkmauth_ bootmode و ساختار security_ops در یک صفحه‌ی فقط خواندنی تحت حفاظت RKP آخرین کاری است که محققان پیشنهاد داده‌اند.

اخبار فنی

وصله آسیب‌پذیری منع سرویس در اندروید از سوی گوگل

یکی از ۷۸ مورد آسیب‌پذیری که در خبرنامه امنیتی اندروید ماه اکتبر گوگل وصله شده است مربوط به یک آسیب‌پذیری در بخش GPS بوده و مهاجمان می‌توانستند از آن برای انجام حملات منع سرویس از راه دور بر روی دستگاه‌های آسیب‌پذیر بهره‌برداری کنند.

یک مهاجم که توانایی دستکاری داده‌های کمکی GPS/ GNSS تولید شده توسط Qualcomm را داشته باشد می‌تواند با بهره‌برداری از این آسیب‌پذیری حملات مرد میانی انجام دهد. گفته می‌شود این اشکال بر روی کد متن‌باز در AOSP و هم‌چنین کد اختصاصی در یک بارگیری‌کننده Java XTRA اثر می‌گذارد.

محققان امنیت سایبری Nighwatch که این آسیب‌پذیری را کشف کرده‌اند توضیح می‌دهند که خبرنامه اندروید ماه اکتبر این اشکال را برطرف کرده است.Qualcomm نیز وصله‌های موردنیاز دیگری را ماه گذشته ارائه کرده بود. البته این محققان می‌گویند سایر بسترهایی که از تراشه‌های GPS متعلق به شرکت Qualcomm استفاده می‌کنند ممکن است تحت تأثیر این آسیب‌پذیری امنیتی باشند.

دستگاه‌هایی که تراشه‌های GPS متعلق به شرکت Qualcomm را دارند به طور مرتب به کارگزارهای OEM متصل می‌شوند تا پرونده‌های کمکی gpsOneXtra را بارگیری کنند. این پرونده‌ها شامل داده‌های مکانی کنونی ماهواره و مکان‌های تقریبی برای ۷ روز آینده است. Qualcomm سامانه gpsOneXtra را در سال ۲۰۰۷ راه‌اندازی کرد. دستگاه‌هایی که از این سامانه استفاده می‌کنند طوری تنظیم شده‌اند که تقریباً هر بار که به شبکه وای‌فای متصل می‌شوند برای پرونده‌های کمکی درخواست بدهند.

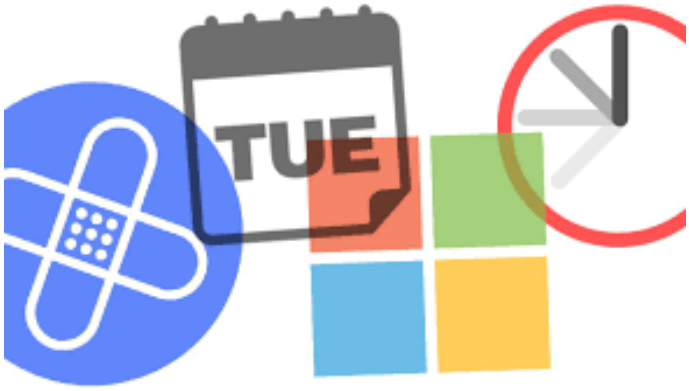
دامنه‌هایی که این دستگاه‌ها به آن‌ها متصل می‌شوند، یعنی gpsonextra(dot)net و izatcloud(dot)net، متعلق به Qualcommبوده و در شبکه انتقال محتوای Amazon's Cloudfront میزبانی می‌شوند (البته به جز یک زیر دامنه). پرونده کمکی توسط یک فرآیند سطح سامانه‌عامل جاوا درخواست می‌شود (GpsXtraDownloader.java). این فرآیند داده را به یک کلاس C++ JNI می‌دهد (com_ android_server_location_GnssLocationProvider. cpp). این کلاس هم پرونده‌ها را در مودم و یا ثابت‌افزار Qualcomm تزریق می‌کند.

این آسیب‌پذیری بر این مبنا استوار است که کد جاوا و یا سی پلاس پلاس بررسی‌های لازم را برای تعیین اندازه پرونده داده انجام نمی‌دهند. این امر موجب می‌شود درصورتی‌که پرونده مذکور از اندازه حافظه باقی‌مانده دستگاه بزرگ‌تر باشد دستگاه ریبوت شود. یک مهاجم به‌طور نظری می‌تواند از طریق اتمام حافظه و اختلال در عملکرد دستگاه، کد دلخواه خود را در مودم Qualcomm و یا سامانه‌عامل اندروید اجرا کند. البته به‌طور عملی

محققـان امنیتـی نتوانسـتند ایـن کار را انجـام دهنـد.
محققـان توضیـح می‌دهنـد: «بـرای انجـام حملـه، یـک مهاجـم مـرد میانـی کـه در جایـی بـر روی شـبکه بیـن دسـتگاه و کارگزارهـای Qualcomm قـرار دارد می‌توانـد از طریـق اسـتراق سـمع درخواسـت‌های ارسـالی تلفن‌همـراه حملـه را آغـاز کـرده و پرونده‌هـای بـزرگ خـود را جایگزیـن آن‌هـا کنـد. ازآنجایی‌کـه مرورگـر پیش‌فـرض نصـب شـده کـروم بـر روی اندرویـد نـوع و مـدل دسـتگاه را نشـان می‌دهـد، انـدازه حافظـه بیشـینه از ایـن اطلاعـات به‌دسـت آمـده و انـدازه پرونـده لازم بـرای حملـه آشـکار می‌شـود.»
یـک عامـل مخـرب می‌توانـد از طریـق مسـیریاب‌های مـورد نفـوذ واقـع شـده و یـا سـایر منابـع حمـلات خـود را ترتیـب دهـد. تنهـا عامـل محـدود کننـده ایـن حملـه ایـن اسـت کـه مهاجـم بایـد از یـک پرونـده بـه بزرگـی حافظـه در دسـترس بـر روی تلفن‌همـراه اسـتفاده کنـد. دسـتگاه‌های اندرویـدی کـه وصلـه امنیتـی 2016-10-01 را اعـمال کرده‌انـد از ایـن حملـه در امـان هسـتند. بـه گفتـه محققـان امنیتـی دسـتگاه‌های GPSدار سـاخته شـده توسـط اپـل (آی‌پـد، آیفـون و غیـره) و هم‌چنیـن مایکروسـافت (دسـتگاه‌های تلفن‌همـراه مایکروسـافت و Surface) تحـت تأثیـر ایـن آسـیب‌پذیری نیسـتند.

اخبار فنی

وصله‌های روز سه‌شنبه: مایکروسافت ۵ آسیب‌پذیری روز-صفرم را وصله کرد



مایکروسافت روز سه‌شنبه 10 بولتن صادر کرد که 45 آسیب‌پذیری شامل 5 آسیب‌پذیری روز-صفرم را پوشش می‌داد. این به‌روزرسانی منطبق با متدلوژی جدید مایکروسافت در به‌روزرسانی‌ها است.

5 مورد از این به‌روزرسانی‌ها جدی، 4 مورد مهم و یک مورد هم متوسط گزارش شده است و چندین محصول مایکروسافت از جمله ویندوز، اینترنت اکسپلورر، Edge و آفیس را شامل می‌شود. مایکروسافت گزارش داد بهره‌برداری از هریک از آسیب‌پذیری‌های جدی می‌تواند منجر به اجرای کد از راه دور شود. 5 آسیب‌پذیری روز-صفرم و جدی با شناسه‌های MS16-118، MS16-119، MS16-120، MS16-121 و MS16-126 شناسایی شده و در دنیای واقعی مورد بهره‌برداری قرار گرفته‌اند.

آمل ساروت، مدیر آزمایشگاه آسیب‌پذیری در Qualys می‌گوید: «به‌طور کلی به‌روزرسانی امنیتی این هفته با اندازه‌ی متوسط B بوده است اما بسیار جدی است چرا که در آن چند وصله‌ی آسیب‌پذیری روز-صفرم مشاهده می‌شود.»

آسیب‌پذیری روز-صفرم MS-118 با شناسه‌ی CVE-2016-3298 آسیب‌پذیری افشای اطلاعات مرورگر مایکروسافت است. MA-119 با شناسه‌ی CVE-2016-7189 یک آسیب‌پذیری اجرای کد از را دور بر روی ماشین اسکریپتی است. MS16-120 با شناسه‌ی CVE-2016-3393 مربوط به آسیب‌پذیری RCE مؤلفه‌های گرافیکی ویندوز است. MS16-121 با شناسه‌ی CVE-2016-7193 آسیب‌پذیری خرابی حافظه در آفیس مایکروسافت است و آخرین آسیب‌پذیری CVE-2016-3298 که در بولتن مایکروسافت با شناسه MS16-126 شناخته می‌شود، آسیب‌پذیری روز-صفرم است که در درجه‌بندی، جدی در نظر گرفته نشده و سطح متوسط دارد. این مورد آسیب‌پذیری افشای اطلاعات در اینترنت اکسپلورر را برطرف می‌کند.

تاد بردسلی، مدیر تحقیقات امنیتی Rapid7، در رایانامه‌ای به SCMagazine.com گفت: «این ماه شاهد آن هستیم که بخش وسیعی از به‌روزرسانی‌های مایکروسافت از مدیران کارگزارها عبور کرده است چرا که بسیاری از وصله‌ها در ماه اکتبر مربوط به سمت کارخواه هستند. تنها استثناء مربوط به MS16-121 است که کارگزار SharePoint را از طریق مایکروسافت آفیس تحت تأثیر قرار می‌دهد. اگر این آسیب‌پذیری وصله‌نشده رها شود، یک مهاجم که قابلیت ذخیره‌سازی اسناد بر روی کارگزار SharePoint را دارد، می‌تواند یک پرونده‌ی جعلی RTF را بارگذاری کرده و بر روی کارگزار تحت تأثیر قرارگرفته، اجرای کد از راه دور (RCE) را بدست آورد.»

به‌روزرسانی روز سه‌شنبه مربوط به ماه اکتبر مایکروسافت، اولین دوره از متدولوژی «ادغام ماهانه» مایکروسافت است که منتشر شده و سامانه‌ای است که

در زمان اعلام شدن به گرمی توسط مدیران صنعتی مورد استقبال قرار نگرفت.

مایکروسافت در ماه آگوست اعلام کرد برای به‌روزرسانی ماه اکتبر خود متدولوژی ادغام ماهانه را برقرار خواهد کرد که شامل مسائل امنیتی و اعتباری به‌طور یکجا خواهد بود، بجای اینکه برخی از به‌روزرسانی‌ها را جداگانه ارائه کند تا مدیران سامانه آن را انتخاب کنند.

مایکروسافت باور دارد که این شیوه‌ی جدید، زندگی را برای ادمین سامانه راحت‌تر خواهد کرد و بدون تکه‌تکه کردن به‌روزرسانی‌ها، ویندوز قابل اطمینان‌تر خواهد شد.

کریگ یانگ، محقق امنیتی Tripwire در رایانامه‌ای به SCMagazine.com گفت: «البته که مهم‌ترین رویداد در به‌روزرسانی این ماه مایکروسافت مربوط به متدولوژی جدید ادغام ماهانه است که برای تمامی سامانه عامل‌های ویندوز تا ویندوز 7 خواهد بود. با این رویکرد رو به جلو، مایکروسافت برای هر بستری دو به‌روزرسانی منتشر خواهد کرد. یکی از این به‌روزرسانی‌ها مسائل و اشکالات امنیتی در ویندوز را برطرف خواهد کرد، در حالی‌که دیگری با عنوان ادغام ماهانه، شامل اشکالات غیرامنیتی ویندوز خواهد بود که قابلیت اطمینان برنامه‌ها را بهبود خواهد داد.»

یانگ همچنین اشاره کرد این شیوه‌ی جدید مایکروسافت در به‌روزرسانی ممکن است مشکلاتی را برای گروه‌های امنیتی به‌وجود آورد. اگر یکی از جنبه‌های این به‌روزرسانی با سامانه‌ی آن‌ها سازگار نباشد، در این موقعیت محققان در شرایط سختی خواهند بود که مجبورند برنامه با نسخه‌ی سازگار را نصب کنند یا سامانه را با همان آسیب‌پذیری رها کنند. مشکل بالقوه‌ی دیگر زمانی است که تمامی به‌روزرسانی‌ها در یک پرونده، بسیار بزرگ شده و بارگیری آن تمام منابع سامانه را خواهد گرفت.

اخبار فنی

هشدار سیسکو در خصوص آسیب‌پذیری‌های جدی در سوئیچ‌های Nexus

سامانه‌ی سیسکو این هفته چند وصله‌ی حیاتی مربوط به سوئیچ‌های Nexus سری 7000 و برنامه‌ی NX-OS منتشر کرد. این آسیب‌پذیری‌ها اجازه‌ی دسترسی به سامانه از راه دور و قابلیت اجرای کد و دستور توسط مهاجم بر روی دستگاه هدف را می‌دهد.

با توجه به راهنمایی امنیتی سیسکو روز چهارشنبه، هر دو سری 7000 و 77000 سوئیچ‌های Nexus در معرض نقص سرریزِ بافر مجازی‌سازی انتقال پوششی هستند.

این اشکال (CVE-2016-1453) به علت اعتبارسنجی ناقص ورودی انجام‌شده بر روی پارامتر سرآیند بسته‌های مجازی‌سازی انتقال پوششی است.

سیسکو می‌گوید، بهره‌برداری از این آسیب‌پذیری، سرریز بافر را در پی خواهد داشت که دری به‌سوی مهاجم باز می‌کند تا کد دلخواه خود را بر روی سامانه‌ی هدف اجرا کرده و کنترل آن را در دست گیرد. سیسکو برای این مسئله به‌روزرسانی‌های نرم‌افزاری را منتشر کرده و دستورات راه‌حلی ارائه داده تا خطرات این آسیب‌پذیری را کاهش دهد.

سیسکو همچنین به آسیب‌پذیری (CVE-2015-0721) دیگری نیز اشاره کرده است که سوئیچ‌های این شرکت را تحت تاثیر قرار می‌دهد. این آسیب‌پذیری با زیرسامانه‌ی پروتکل SSH استفاده شده در سوئیچ‌های Nexus سیسکو، گره خورده است و می‌تواند به یک مهاجم غیرمجاز و راه دور اجازه دهد تا احراز هویت، دسترسی به مجوز و حسابرسی (AAA) را دور بزند.

سیسکو می‌نویسد: «تحت شرایط خاص، با یک بهره‌برداری موفق مهاجم می‌تواند محدودیت‌های AAA را دور زده و بر روی واسط خط فرمان قربانی دستوراتی را اجرا کند که این امتیازات به نقش‌های کاربری مختلفی اعطا شده است.» سیسکو در ادامه می‌گوید به‌روزرسانی‌های نرم‌افزاری را برای اشاره به این آسیب‌پذیری منتشر کرده است ولی تاکنون راه‌حلی برای این مسئله ارائه نکرده است.

برخی مشاوره‌های کمتر قابل توجه سیسکو با درجه‌ی اهمیت بالا ارائه شده است که هر یک مربوط به سامانه عامل این شرکت با نام NX-OS است.

اولین آسیب‌پذیری (CVE-2016-1454) مربوط به پروتکل دروازه‌ی مرزی و با هدف منع سرویس است. بنا به گفته‌های سیسکو، با استفاده از این آسیب‌پذیری و بخاطر بارگیری مجدد و غیرمنتظره‌ی دستگاه، یک مهاجم غیرمجاز و از راه دور می‌تواند شرایط حمله‌ی منع سرویس را بوجود آورد.

دو آسیب‌پذیری باقی‌مانده که توسط سیسکو نرخ خطر بالایی گرفته‌اند مربوط به مؤلفه‌های DHCPv4 در سامانه عامل NX-OS است. به همین ترتیب، هر دوی این آسیب‌پذیری‌ها شرایط حمله‌ی منع سرویس را فراهم می‌آورند.

بنا به گزارش‌های سیسکو یکی از این آسیب‌پذیری‌ها (CVE-2015-6392) ناشی از پیاده‌سازی رله‌ی DHCPv4 و عامل رله‌ی هوشمند در نرم‌افزار NX-OS است. سیسکو می‌گوید: «آسیب‌پذیری ناشی از اعتبارسنجی نامناسب بسته‌های پیشنهادی و جعلی DHCPv4 است. یک مهاجم با ارسال بسته‌های جعلی پیشنهادی DHCPv4 به دستگاه هدف، از این آسیب‌پذیری بهره‌برداری می‌کند. این بهره‌برداری توسط مهاجم باعث درهم‌شکستگی DHCP و یا دستگاه می‌شود.

سیسکو می‌گوید این آسیب‌پذیری تنها با ارسال بسته‌های IPv4 مورد بهره‌برداری قرار بگیرد.

بنا به گزارش سیسکو، دومین آسیب‌پذیری (CVE-2015-6393) مربوط به DHCPv4 با نرم‌افزار NX-OS سیسکو گره خورده است و با استفاده از ارسال بسته‌های ناقص DHCPv4 مهاجم از راه دور می‌تواند بر روی دستگاه هدف شرایط جمله‌ی منع سرویس را فراهم آورد.

بنا به گفته‌ی سیسکو، در یک سناریو مهاجم می‌تواند با ارسال بسته‌ی ناقص DHCP که توسط عامل رله‌ی DHCP بر روی سامانه‌ی قربانی به گوش است، موجب بهره‌برداری از این آسیب‌پذیری شود. این بسته‌ی ناقص DHCP می‌تواند به آدرس IP همه‌پخشی یا تک‌پخشی قربانی بر روی یکی از واسط‌ها ارسال شود. این شرایط و این سناریو باعث درهم‌شکستگی فرآیند DHCP و یا دستگاه قربانی می‌شود.

برای هر دو آسیب‌پذیری DHCPv4 سیسکو به‌روزرسانی نرم‌افزاری منتشر کرده است ولی هنوز راه‌حلی برای این مشکلات در دسترس نیست.

فصل پنجم

اخبار تحـــلیلی

اخبار تحلیلی

آلودگی بیش از ۱۰۰ فروشگاه برخط به بدافزار جدید Magecart

بیش از ۱۰۰ فروشگاه برخط مورد آماج حملات گونه‌ی تازه‌ای از بدافزارهای تحت وب واقع شده که Magecart نام دارد، این بدافزار به‌طور مخفیانه اطلاعات واردشده به صفحات پرداخت را دزدیده و آن‌ها را به کارگزار نفوذگر می‌فرستد.

نخستین نشانه‌های این بدافزار در ماه مارس ۲۰۱۶ رؤیت شد، اما فعالیت‌های آن در ماه می توجه محققان را جلب کرد، درست زمانی که برای اولین بار این آلودگی در فروشگاه‌های برخط محبوب منتشر شد.

در اواخر ژوئن ۲۰۱۶، سوکوری با یک گونه از Magecart برخورد کرد که بنا به گزارش‌های Softpedia فروشگاه‌های Magento را هدف قرار داده بود؛ فروشگاه‌های Magento از افزونه‌ی Braintree Magento برای پشتیبانی از پرداخت‌ها از طریق بستر Braintree استفاده می‌کند.

Magecart می‌تواند سامانه‌های مدیریت محتوای تجارت الکترونیک را هدف قرار دهد

در واقع، این تنها یک جنبه از حمله‌ی Magecart بود، که شرکت‌هایی مانند ClearSky و RiskIQ در چندین بستر خرید برخط به پی‌گیری آن پرداخته‌اند.

از ماه مارس گروه پشت پرده‌ی کمپین Magecart قابلیت‌های خود را افزایش داده است، اسکریپت‌های مخرب خود را به منظور اجرا در سراسر سامانه‌هایی هم‌چون OpenCart، Magento، و Powerfront اصلاح نموده است.

این بدافزار چیزی بیش از یک پرونده‌ی جاوااسکریپت نیست که به کد منبع وب‌گاه تحت نفوذ اضافه شده است. این اتفاق زمانی می‌افتد که نفوذگر از یک آسیب‌پذیری در سامانه‌ی مدیریت محتوا یا خود کارگزار سوءاستفاده کند. هرگاه نفوذگر به بستر مدیریت محتوا یا کارگزار زیرساخت آن دسترسی داشته باشد، کد مخرب خود را به کد منبع وب‌گاه می‌افزاید.

Magecart فقط در صفحات پرداخت فعال می‌شود

آلودگی‌های Magecart در دو مرحله اتفاق می‌افتند؛ در گام او اسکریپت مورد نظر بررسی می‌کند که آیا کاربر در صفحه‌ی پرداخت قرار دارد یا خیر. فقط وقتی که کاربر به URL مخصوص صفحه‌ی پرداخت هر سامانه دست پیدا می‌کند، اسکریپت Magecart به مرحله‌ی دوم وارد می‌گردد، جایی که مؤلفه‌ی کی‌لاگر واقعی را بارگذاری می‌نماید.

اسکریپت Magecart شامل یک فروشگاه تجارت الکترونیک زنده است.

این مؤلفه‌ی مرحله‌ی دوم یک اسکریپت JS دیگر است، بدین معنا که از هرآن‌چه که کاربر در فیلدهای فرم وارد کند گزارش تهیه کرده و داده‌های جمع‌آوری‌شده را به یک کارگزار راه دور تحت کنترل نفوذگر می‌فرستد.
این اسکریپت‌ها از دامنه‌های بارگذاری می‌شوند که آلودگی آن‌ها متفاوت است، به این معنا که کلاه‌برداران سایبری می‌دانند که چگونه بایست ردپای خود را مخفی نگه دارند. تمامی اسکریپت‌ها به وسیله‌ی HTTPS بارشده و داده‌ها تیز توسط HTTPS فیلتر می‌شوند.
در مواردی که فرم پرداخت تمامی اطلاعات مورد نظر نفوذگر را گردآوری نمی‌کند، Magecart می‌تواند فیلدهای ورودی را به فرم پرداخت وب‌گاه اضافه کند تا به این روش همه‌ی داده‌های مد نظر نفوذگر جمع‌آوری شود.

بیش از ۱۰۰ فروشگاه تحت تأثیر این بدافزار قرار گرفته‌اند
RiskIQ می‌گوید که Magecart می‌تواند داده‌هایی را از فروشگاه‌های برخطی برباید که خودشان مسئول رسیدگی به عملیات پردازش پرداختشان هستند، یا فروشگاه‌هایی که این پردازش را به ساز و کارهای تخصصی پرداخت می‌سپارند.
RiskIQ می‌گوید که Magecart قادر بوده اطلاعات مندرج در کارت اعتباری را از وب‌گاه‌هایی به سرقت ببرد که از افزونه‌ی Braintree Magento استفاده می‌کنند یا پرداخت‌ها را به وسیله‌ی VeriSign مدیریت می‌نمایند.
بعضی از مهم‌ترین شرکت‌های محبوب که از آلودگی فروشگاه‌های برخطشان به Magecart آسیب دیده‌اند شامل Everlast و Faber & Faber است.
راحت‌ترین راه برای حفاظت مقابل آلودگی‌های ناشی از Magecart استفاده از اطلاعات محرمانه و پیچیده‌ی مدیر وب‌گاه و نیز به‌روز نگه داشتن کارگزار و نرم‌افزار مدیریت محتواست.

اخبارتحلیلی

کمپین هرزنامه‌ی آلوده به بدافزار Eko کاربران فرانسوی را هدف حمله قرار داده است

یک کمپین هرزنامه‌ی فیس‌بوک فعالیت‌های گسترده‌ای را در فرانسه ترتیب داده است؛ ابعاد این حمله به اندازه‌ای بوده که بعد از سر به فلک کشیدن میزان آلودگی‌های ناشی از این کمپین هرزنامه، مقامات دولتی این کشور هفته‌ی گذشته اقدام به صدور یک اخطار رسمی کرده‌اند.

این کمپین طوری وانمود می‌کند که کاربران پیامی را از سوی یکی از دوستان خود دریافت کرده‌اند، و از آن‌ها می‌پرسد که آیا آن‌ها در ویدئوی ارسالی حضور دارند یا خیر.

پیوند موجود در هرزنامه منجر به رسیدن به یک فیلم بارگذاری‌شده در یوتیوب می‌شود.

این پیام به خوبی طراحی شده تا بتواند هم از اسم گیرنده و هم از عکس وی در پیش‌نمایش پیوند هرزنامه استفاده نماید.

کاربرانی که این پیوند را دنبال می‌کنند، فریب می‌خورند و یک افزونه‌ی مربوط به مرورگر کروم را نصب می‌نمایند تا فیلم مورد نظر نمایش داده شود. بدافزار Eko در پس این افزونه قرار دارد.

براساس گزارشی مندرج در رسانه‌های محلی فرانسه نظیر روزنامه‌ی لوموند، این افزونه که دارای اسامی مختلفی می‌باشد، تبلیغات را در صفحه‌ای تزریق می‌کند که کاربران از آن بازدید می‌نمایند، همچنین می‌تواند داده‌هایی مانند گذرواژه و تاریخچه‌ی مرورگر را جمع‌آوری کند.

در حال حاضر فیس‌بوک این‌گونه پیام‌ها را پویش و مسدود می‌کند. در سه‌شنبه، ۴ اکتبر، وزارت کشور فرانسه از طریق صفحه‌ی فیس‌بوک خود به کاربران هشدار داد که هرگز روی چنین پیوندهایی کلیک نکنند.

کاربرانی که روی این پیوندها کلیک کرده‌اند می‌بایست تنظیمات مرورگر خود را زیر و رو کنند و این افزونه‌ی جعلی را پاک نمایند. مقامات می‌گویند که کاربران سایر مرورگرها هم ممکن است در معرض چنین افزودنی‌های مخربی قرار داشته باشند.

تا بدین لحظه‌ای هیچ خبری مبنی بر این‌که کاربران سایر کشورها تحت تأثیر این کمپین هرزنامه قرار گرفته‌اند منتشر نشده است.

اخبار تحلیلی

مرد میانی واقعی: انتقال جزئیات ورود از طریق بدن انسان

محققان علوم رایانه در دانشگاه واشنگتن در حال توسعه فناوری هستند تا داده‌ها را به‌جای استفاده از رسانه‌های سیمی و یا هوا به شیوه امنی از طریق بدن انسان ارسال کنند.

کلمات‌عبوری که از طریق شبکه‌های ناامن ارسال می‌شوند به‌راحتی استراق سمع می‌شوند. می‌توان با استفاده از فناوری VPN با این مشکل مقابله کرد؛ اما حالا محققان امنیتی رویکردی متفاوت را در مشکلی مشابه پیش گرفته‌اند که از آسیب‌پذیری‌های پروتکل‌های رادیویی مورد استفاده در دستگاه‌های پوشیدنی و کار گذاشته شده محافظت می‌کند.

این فناوری در تلفیق با حسگرهای اثرانگشت در گوشی‌های هوشمند کار می‌کند. برای مثال یک قفل در هوشمند را در نظر بگیرید. یک کاربر می‌تواند به‌طور همزمان دستگیره در را در یک سو و حسگر اثرانگشت تلفن‌همراه خود را در سوی دیگر لمس کند، بدین‌ترتیب جزئیات ورود به جای هوا از طریق بدن منتقل می‌شوند. به نقل از مقاله منتشر شده توسط این محققان این فناوری محدود به نوع خاصی از بدن و یا حالت ایستادن خاصی نیست: «ما برای اولین بار نشان دادیم که می‌توان از دستگاه‌هایی که مبتنی بر انتقال بی‌سیم هستند از طریق بدن انسان بهره ببریم. به‌علاوه نشان داده‌ایم که دستگاه‌هایی مانند حسگر اثرانگشت و پدهای لمسی برای گیرنده‌های بی‌سیمی نیز کار می‌کنند که در تماس با بدن باشند. در این پژوهش انتشار داده‌ها را در بدن انسان بررسی کردیم و با 10 فرد مختلف آزمایش‌ها را انجام دادیم تا نشان دهیم این روش به نوع خاصی از بدن و یا حالت ایستادن وابسته نیست. در این پژوهش توانستیم به نرخ بیت ۵۰ بیت بر ثانیه از طریق بدن انسان دست یابیم.»

این روش در حسگرهای اثرانگشت به‌خوبی کار می‌کند چرا که این حسگرها سیگنال‌های الکترومغناطیسی با فرکانس کم‌تر از ۱۰ مگاهرتز را تولید می‌کنند که به‌خوبی از طریق بدن انسان منتقل می‌شوند.

این محققان می‌گویند چندین آزمایش را با حسگرهای آیفون 6S و 5S، پویشگرهای اثرانگشت Verifi P5100 USB و پدهای لمسی مدل‌های Adafruit و T440s از شرکت لنوو انجام داده‌اند. به گفته محقق امنیتی بیل کامارادا تداخل دستگاه‌های پوشیدنی و دستگاه‌های فلزی مانند ساعت مشکل جدی در این آزمایش‌ها ایجاد نکرده است، اما مشکل اصلی نرخ ارسال ۲۵ بیت بر ثانیه است که حتی کم‌تر از مودم‌های ۱۹۵۰ است. این محقق می‌گوید هنوز راه زیادی از آزمایشگاه تحقیقاتی تا عملیاتی شدن این پروژه در بدن انسان وجود دارد اما اگر این اتفاق بیفتد کاربردهای مختلفی دارد. به عنوان مثال به‌جای نوشتن دستی کلمه‌عبور برای مرتبط ساختن دستگاه‌های پزشکی مانند نظارت‌کننده سطح فشار و یا قند خون با

گوشی هوشمند، امکان انتقال کلیدهای رمز از طریق بدن انسان فراهم می‌شود.

این محقق خاطر نشان کرده است که استفاده از بدن انسان به‌عنوان رسانه انتقالی داده‌ها نگرانی‌های جدید امنیتی را درباره حملات مرد میانی ایجاد خواهد کرد.

اخبار تحلیلی

به لطف موتور جستجوی Shodan بستر خدمات باج‌افزاری Encryptor غیرفعال شد

متخصصان امنیتی می‌گویند توانسته‌اند معماری یک نمونه باج‌افزار به‌عنوان خدمت را با نام Encryptor شناسایی کنند.

موتور جستجوی Shodan یک جستجوگر برای دستگاه‌های متصل به اینترنت است که متخصصان فناوری اطلاعات و البته نفوذگرها از آن برای ارزیابی سامانه‌های متصل به اینترنت استفاده می‌کنند. اطلاعات به دست آمده از این موتور جستجو به نفوذگران امکان می‌دهد سامانه‌های برخطی را که آسیب‌پذیر هستند شناسایی کرده و به آن‌ها حمله کنند.

از طرف دیگر نمی‌توان قابلیت‌های این موتور جستجو را در مقابله با باتنت‌ها دست‌کم گرفت. در فصل تابستان متخصصان امنیتی به کمک مقامات توانستند از Shodan برای غیرفعال‌سازی باتنت باج‌افزار به‌عنوان خدمت Encryptor که برای توزیع باج‌افزارها استفاده می‌شد بهره ببرند.

این باتنت، باج‌افزار را در قالب خدمت ارائه می‌کرد بدان معنا که به مجرمان اجازه می‌داد بدون داشتن دانش خاصی بدافزارهای خود را ساخته و آن‌ها پخش کنند. مدل فروش فراهم شده در این بستر به مجرمان سایبری امکان می‌داد بدافزار را ساخته، زیرساخت مورد نیاز را برای پیاده‌سازی این بدافزار اجاره کرده و پرداختی‌های قربانیان را دریافت کنند.

ترندمیکرو در این خصوص می‌گوید: «بستر باج‌افزار به‌عنوان خدمت Encryptor یک پنل تحت وب را برای کاربران خود آماده کرده است که فقط از طریق Tor قابل‌دسترس بوده و به آن‌ها امکان مدیریت سامانه‌های قربانیان را می‌دهد. در این سامانه از واحد پول بیت‌کوین استفاده می‌شود. در مقایسه با سایر باج‌افزارها مانند Cerber که توسعه‌دهندگان ۴۰ درصد سهم دریافت می‌کنند این بستر به‌صرفه‌تر است. فروشندگان باج‌افزار باید حداقل ۵ درصد فروش خود را بپردازند تا توزیع باج‌افزار خود را ادامه دهند.»

Encryptor اولین بار در سال ۲۰۱۵ کشف شد، اما متخصصان Cylance در ماه مارس متوجه افزایش چشم‌گیر قربانیان این بستر شدند. آن‌ها در این زمان ۱۸۱۸ مورد قربانی را کشف کردند.

Cylance دراین‌باره می‌گوید: «باج‌افزار به عنوان خدمت Encryptor از اواسط سال ۲۰۱۵ درحال فعالیت بوده است. این باج‌افزار فقط از طریق دامنه .onion بر روی شبکه Tor قابل دسترس است. نویسنده باج‌افزار ۲۰ درصد مبلغ باج دریافت‌شده را برای خود می‌گیرد. تعداد قربانیان

تابه‌حال ۱۸۱۸ مورد بوده که از این میان ۸ مورد باج درخواستی را پرداخت کرده‌اند.»

مجرمان پشت این باج‌افزار به‌عنوان خدمت، از این بستر به‌عنوان «کاملاً غیرقابل شناسایی» یاد می‌کنند و البته به نظر می‌رسد ادعای آن‌ها نامربوط هم نباشد، چرا که بر اساس گزارش ارائه شده توسط پویشگر ویروس برخط NoDistribute، ۲ مورد از ۳۵ مورد ضدویروس توانایی شناسایی این تهدید را دارند.

متخصصان امنیتی با بهره‌گیری از ویژگی‌های پیاده‌سازی شده در Shodan توانسته‌اند یکی از کارگزارهای Encryptor را کشف کنند. آن‌ها می‌گویند این کارگزار به جای این‌که در شبکه Tor مخفی باشد، خوب تنظیم نشده و به اینترنت متصل بوده است.

مقامات کارگزار مذکور را ضبط کرده و طی چند روز مکان ۳ ماشین دیگر را نیز کشف کردند.

ترندمیکرو درباره این کشف می‌گوید: «در جریان بررسی‌ها مشخص شد که یکی از کارگزارهای دستور و کنترل این باج‌افزار در اینترنت در دسترس همگان قرار گرفته است. Shodan میزبانی این باج‌افزار را در یک بستر خدمات ابری نشان می‌داد. در اواخر ماه ژوئن سامانه‌های مربوطه توسط مقامات ضبط و غیرفعال شدند.»

اخبار تحلیلی

آسیب‌پذیری بیش از ۵۰۰ هزار دستگاه اینترنت اشیاء به باتنت Mirai

محققان امنیتی می‌گویند ۵۰۰ هزار دستگاه اینترنت اشیاء را کشف کرده‌اند که در برابر باتنت Miraiو یا باتنت‌های مشابه آسیب‌پذیر هستند.

اخیراً باتنت Mirai و حداقل یک نمونه باتنت دیگر (BASHLITE) به‌عنوان عوامل اصلی حملات منع سرویس توزیع‌شده به وبگاه روزنامه‌نگار امنیتی برایان کربز و خدمات میزبانی OVH شناخته شدند. حمله صورت گرفته علیه OVHحتی به یک ترابیت بر ثانیه هم رسیده بود. بسیاری از شرکت‌های امنیتی معتقدند حملاتی چنین گسترده و با این مقیاس عظیم احتمالاً توسط دستگاه‌های اینترنت اشیای مورد نفوذ واقع‌شده، به‌خصوص دوربین‌ها و DVRها انجام شده‌اند. محققان امنیتی می‌گویند اکثر این دستگاه‌ها جزئیات ورود ضعیف و یا پیش‌فرض دارند. نویسنده باتنت Mirai کد منبع آن را منتشر کرده و مدعی شده است که به‌اندازه کافی از این ساخته خود پول به جیب زده است. کد منبع منتشر شده شامل ۶۰ ترکیب نام‌کاربری و کلمه‌عبور بوده است که باتنت Mirai برای نفوذ به دستگاه‌های اینترنت اشیاء استفاده می‌کرده است.

یکی از این ترکیبات root/xc3511 است و محققان امنیتی Flashpoint کشف کرده‌اند که دستگاه‌های اینترنت اشیایی که این نام کاربری و کلمه‌عبور را داشته‌اند سهم قابل توجهی در باتنت Mirai داشته‌اند.

متخصصان می‌گویند محصولات نظارت ویدئویی متعلق به شرکت Dahua بیش‌ترین میزان دستگاه‌های مورد نفوذ واقع‌شده را تشکیل می‌دهند. بسیاری از سازندگان دستگاه‌های دوربین IP، DVR و NVR بخش‌های مختلف نرم‌افزاری و سخت‌افزاری خود را از یک شرکت چینی با نام XiongMai می‌گیرند. شرکت مذکور نرم‌افزار آسیب‌پذیری را تولید می‌کند که در حداقل یک میلیون دستگاه کار گذاشته شده است.

مادامی‌که این دستگاه‌ها به اینترنت متصل نباشند این حقیقت که در بسیاری از آن‌ها از نام‌کاربری و کلمه‌عبور پیش‌فرض استفاده شده است نمی‌تواند خیلی نگران‌کننده باشد. مشکل اینجاست که ثابت‌افزار تولید شده توسط شرکت چینی مذکور شامل یک سرویس telnet نیز می‌شود که به‌صورت پیش‌فرض فعال است. این سرویس دسترسی از راه‌دور را به دستگاه‌ها به‌سادگی میسر می‌سازد. بدتر این‌که جزئیات ورود پیش‌فرض قابل تغییر نیستند چرا که در خود کد برنامه ثبت شده‌اند. غیرفعال‌سازی سرویس telnet نیز کار سختی است.

یک پویش اینترنتی انجام شده توسط Flashpoint با استفاده از موتور جستجوی Shodan نشان می‌دهد که بیش از ۵۰۰ هزار دستگاه وجود دارند که در برابر هردوی این اشکال‌ها آسیب‌پذیر بوده و هدف مناسبی برای Mirai و سایر باتنت‌ها محسوب می‌شوند.

کشورهایی که بیش‌ترین دستگاه‌های آسیب‌پذیر را

دارند شامل ویتنام (۸۰ هزار)، برزیل (۶۲ هزار)، ترکیه (۴۰ هزار)، تایوان (۲۹ هزار)، چین (۲۲ هزار)، کره‌جنوبی (۲۱ هزار)، تایلند (۱۶ هزار)، هندوستان (۱۵ هزار) و انگلیس (۱۴ هزار) بوده‌اند.

Flashpointمی‌گوید درحالی‌که باتنت Mirai بسیاری از دستگاه‌های Dahua را مورد نفوذ قرار داده است، بخش قابل‌توجهی از IPهای استفاده شده در حملات اخیر منع از سرویس توزیع‌یافته به محصولات XiongMai بازمی‌گردند. متخصص امنیتی زاک ویکهلم، می‌گوید ۶۵ Dahua درصد آلودگی‌ها را در آمریکا شامل می‌شود و دستگاه‌های XiongMai نیز ۷۰ درصد آلودگی‌ها را در کشورهایی هم‌چون ویتنام و ترکیه تشکیل می‌دهند. ویکهلم می‌گوید ترکیب root/xc3511 که در فهرست Mirai در صدر است نشان می‌دهد مجرمان سایبری می‌دانند این دستگاه‌ها محبوب هستند.

اخبار تحلیلی

فراتر از تشخیص مبتنی بر امضاء

نفوذ سایری همچنان بدون هیچ انتهایی ادامه دارد و صنعت امنیت به دنبال روش‌های جدیدی برای مقابله با این تهدیدها است. برخی از جناح‌ها ادعا می‌کنند که به اشتراک‌گذاری امضاءهای بهبودیافته می‌تواند راه‌حل اصلی باشد، درحالی‌که برخی دیگر معتقدند امضاءها مرده‌اند. واقعیت این است تا زمانی که امضاءها به‌عنوان یک مؤلفه‌ی اصلی برای تشخیص و پیشگیری از تهدیدات و حملات شناخته‌شده باقی بمانند، این روش‌ها برای مقابله با حملات مدرن کافی نخواهد بود.

امضاءها به‌عنوان پزشکان امنیتی قابلیت تشخیص و جستجو برای آثار مرتبط با پویش‌های قبلاً شناخته‌شده، پاسخ‌دهی به نفوذهای خارجی و تشخیص سامانه‌های دیگری که تحت این نفوذ قرار گرفته‌اند، ارائه می‌کند. هرچند تکنیک تهدیدهای مدرن و جدید به سرعت در حال تغییر است. ارتباطات مهاجمان به‌طور رمزنگاری شده صورت می‌گیرد. بدافزارها برای هر قربانی سفارشی شده و زیرساخت‌های کمی برای حمله استفاده شده و هر زیرساخت به‌کار رفته به سرعت به چرخه باز می‌گردد. علاوه بر این، تکنیک‌های غیربدافزاری، همچون استفاده از اعتبارنامه‌های قانونی و سوءاستفاده از ابزارهای مدیریت قانونی رو به افزایش است. با همه‌ی این‌ها، امضاءها برای تشخیص و اصلاح حملات مدرن کافی نیستند.

امضای بهتر و به‌اشتراک‌گذاری قوی‌تر پاسخ این مشکل نیست. صنعت امنیت نیازمند روش‌های تشخیص قوی و پیچیده‌تر برای مقابله علیه مهاجمان است. ما به‌طور همزمان باید نقاط مخفی سطح پایین سامانه عامل را نیز کنترل کنیم تا بتوانیم الگوهای مرتبه-بالاتر از داده‌های جمع‌آوری شده در سطح شبکه داشته و فعالیت‌های مشکوک و غیرعادی را تشخیص دهیم. همچنین در کنار آن می‌توان از روش‌های تشخیص مبتنی بر امضاء نیز به‌عنوان شانس بیشتری برای تشخیص حمله استفاده کرد. فرضیه‌ی اساسی برای صنعت امنیت امروز این است که نیاز به کار بیشتر وجود دارد. حرکت از استفاده‌ی صرف از تشخیص مبتنی بر امضاء به سمت تشخیص الگو و رفتار مهاجم بهترین راه برای بیشینه کردن شانس مدافع و کم کردن خطرات و صدمات است.

اخبار تحلیلی

وب‌گاه‌های هک‌شده‌ی وردپرس، کاربران را به سمت فروش کلید ویندوز هدایت می‌کنند!

محققـان در شرکـت امنیتـی Sucuri افزایـش وب‌گاه‌هـای آلـوده‌ای را کنـترل می‌کننـد کـه بازدیدکننـدگان آن‌هـا بـه سـمت دامنه‌هایـی کـه کلیدهـای ویـنـدوز را بـه فـروش می‌رسـاند، هدایـت می‌شـوند.

روز چهارشـنبه در پسـت جدیـدی، ایـن شرکـت امنیتـی جزئیات بررسـی خـود در رابطـه بـا یـک وب‌گاه وردپـرس را کـه نامـی از آن نـبرد، گـزارش داد. پرونده‌هـای اصلـی ایـن وب‌گاه بـرای ایـن منظـور هـک شـده اسـت. همچنیـن در ایـن حملـه بـرای جلوگیـری از تشـخیص توسـط ماشـین‌های جسـتجو، کـد تزریقـی نیـز طراحـی شـده اسـت تـا ایـن وب‌گاه‌هـا در فهرسـت سـیاه ایـن ماشـین‌ها قـرار نگیـرد و بـه کاربـران در خصـوص ایـن هـک هشـداری داده نشـود.

در ایـن نمونـه، بـه کاربرانـی کـه از ایـن دامنه‌هـای مخـرب بازدیـد می‌کننـد، بارگیـری تولیدکننـده‌ی کلیـد ویـنـدوز 8.1 بـرای سـال 2106، بـرای فـروش پیشـنهاد داده می‌شـود.

تحلیلگـر بدافـزار و رهـبر تیـم Bruno Zanelato در ایـن پسـت نوشـته اسـت: «مهاجـمان بـرای اینکـه ایـن پویـش برایشـان سـودآور باشـد، بایـد کاری کننـد کـه محتـوای هرزنامـه بـرای ماشـین‌های جسـتجو غیرقابـل مشـاهده باشـد. بـرای اینکـه از دیـده شـدن ایـن محتـوای مخـرب توسـط گـوگل ممانعـت بـه عمـل آیـد، کـد سـعی می‌کنـد تـا از کشـف شـدن دور بمانـد.»

اخبار تحلیلی

بدافزار جاوا اسکریپت رایانه‌ی شما را خاموش خواهد کرد، اگر به فرآیند مربوط به آن خاتمه دهید

محققان گروه امنیتی Kahu با بدافزاری مواجه شدند که با جاوا اسکریپت کد زده شده است. این بدافزار صفحه‌ی خانگی مرورگر شما را به سرقت برده و اگر شما این نفوذ را تشخیص دهید و سعی در خاتمه دادن به فرآیند آن داشته باشید، کامپیوتر شما را خاموش خواهد کرد.

از سال 2014 انواعی از این بدافزار به‌طور برخط مورد بررسی قرار گرفته است اما هیچ یک رفتار تهاجمی همچون این نسخه‌ی آخر نداشته‌اند.

این بدافزار از طریق پرونده‌های مخرب ضمیمه‌شده در هرزنامه‌ها وارد کامپیوتر کاربر می‌شود و در حالی‌که یک پرونده‌ی جاوا اسکریپت است، در داخل مرورگر اجرا نشده و در میزبان اسکریپت ویندوز، یک اجراکننده‌ی جاوا اسکریپت در ویندوز، اجرا می‌شود.

اقدامات مخرب تحت مبهم‌سازی شدید انجام می‌شود. اگر یک کاربر عادی به کد منبع این بدافزار نگاهی بیندازد، جز نویسه‌های تصادفی درهم و برهم چیزی مشاهده نخواهد کرد.

محققان امنیتی Kahu می‌گویند، بر روی این اسکریپت مبهم‌سازی صورت گرفته تا بار داده‌ی صحیح را مخفی کند، بار داده‌ای که تلاش دارد، بخشی از تنظیمات سطح پایین سامانه عامل را عوض کند. علاوه بر مبهم‌سازی، این بدافزار از تکنیک‌هایی همچون نویسه‌های کدگذاری‌شده، جستجوی عبارات منظم، جایگزینی با عبارات منظم، تبدیل پایه‌ی غیرمعمول و عبارات شرطی استفاده می‌کند.

زمانی که محققان امنیتی پس از بررسی کد منبع آشفته، سعی در مبارزه با این بدافزار داشتند، کشف کردند که بدافزار گام‌های زیر را طی می‌کند:

۱. یک پوشه‌ی جدید در دایرکتوری AppDataRoaming ایجاد کرده و با ایجاد یک کلید رجیستری خود را مخفی می‌نماید.

۲. رونوشتی از برنامه‌ی قانونی wscript.exe ویندوز را داخل این پوشه قرار داده و یک نام تصادفی به آن تخصیص می‌دهد.

۳. بدافزار رونوشت خود را داخل این پوشه قرار داده و یک کلید میانبر نیز برای آن ایجاد می‌کند. نام آن را Start گذاشته و آن را در پوشه‌ی Startup قرار می‌دهد که از طریق منوی شروع ویندوز قابل دسترسی است.

۴. بر روی پرونده‌ی میانبر Start یک آیکون جعلی پوشه قرار می‌دهد تا کاربر فکر کند که پرونده نیست و یک پوشه است.

۵. ادامه‌ی اسکریپت تلاش دارد بررسی کند که آیا اتصال به اینترنت وجود دارد یا خیر. این تلاش با ارتباط به وب‌گاه مایکروسافت، گوگل و بینگ انجام می‌شود.

۶. داده‌ها را به آدرس urchintelemetry[.]com ارسال کرده و یک پرونده‌ی رمزنگاری‌شده را از 95.153.31.22 بارگیری کرده و اجرا می‌کند.

۷. پرونده‌ی رمزنگاری‌شده، جاوا اسکریپت دیگری است که صفحه‌ی خانگی مرورگرهای کروم، اینترنت اکسپلورر و فایرفاکس را به آدرس login.hhtxnet[.]com تغییر می‌دهد که کاربر را به سمت وب‌گاه portalne[.]ws هدایت می‌کند.

۸. این اسکریپت آخر از ابزار مدیریت ویندوز (WMI) برای بررسی محصولات امنیتی استفاده می‌کند.

۹. اگر بدافزار وجود محصولات امنیتی را تشخیص دهد، با نمایش پیام خطای جعلی، به اجرای خود پایان خواهد داد.

۱۰. اگر کاربر برنامه‌ی wscript.exe را در بخش مدیر وظایف ویندوز بررسی کرده و تلاش کند تا آن را خاتمه دهد، اسکریپت یک دستور CLI را اجرا خواهد کرد که باعث خاموش شدن کامپیوتر کاربر می‌شود.

۱۱. اگر کاربر کامپیوتر را مجدداً راه‌اندازی کند، بخاطر اینکه اسکریپت Start در بخش منوی شروع قرار گرفته، بدافزار جاوا اسکریپت مخرب تمام عملیات خود را از سر خواهد گرفت.

داریل، کارشناس امنیت Kahu می‌نویسد: «اگر دیدید که کامپیوتر شما در اثر این اسکریپت مخرب، خاموش شد، به راحتی با راه‌اندازی مجدد کامپیوترتان در حالت امن، از شر این بدافزار خلاص شوید. در حالت امن می‌توانید پیوند مربوط به پرونده‌ی مخرب را از startup حذف کنید. همچنین اگر می‌خواهید این بدافزار را در زمان اجرا تحلیل کنید، به راحتی ابزارهای امنیتی خود را به نام‌های بی‌خطر تغییر دهید.»

اخبارتحلیلی

باج‌افزار WildFire تحت عنوان باج‌افزار جدید Hades Locker احیاء شده است!

عوامل باج‌افزار WildFire، باج‌افزاری که اوایل امسال ظاهر شد، بعد از اینکه محققان امنیتی ابزارهای رمزگشایی آن را تهیه کردند، تصمیم گرفته‌اند آن را با نام تجاری جدید ارائه کنند.

جزئیات باج‌افزار WildFire در اواخر ماه آگوست تشریح شد، زمانی که محققان امنیتی کارگزار دستور و کنترل آن را تصاحب کرده و به کلیدهای رمزگشایی آن دست یافتند. قبلاً بسیاری از کاربران باج را پرداخته کرده بودند که تخمین زده می‌شود پرداختی بالغ بر 80 هزار دلار برای عاملان این بدافزار به دنبال داشته باشد.

اگرچه کارگزار دستور و کنترل این بدافزار آلوده شد ولی عوامل پشت آن هنوز دستگیر نشده‌اند و برنامه‌ریزی می‌کنند تا محصول خود را دوباره با نام تجاری Hades Locker برگردانند. علاوه بر این، بدافزار نسخه‌ی جدید با رمزنگاری بهبودیافته وارد عرصه شده است.

به محض اینکه این باج‌افزار بر روی کامپیوتر قربانی اجرا می‌شود، باج‌افزار برای آدرس IP و مکان جغرافیایی قربانی به آدرس http://ip-api(dot)com/xml متصل می‌شود. سپس بدافزار شناسه‌ی منحصربفرد قربانی، شناسه‌ی ردیابی، نام کامپیوتر، نام کاربری، کشور و آدرس IP قربانی را برای یکی از کارگزارهای دستور و کنترل ارسال می‌کند که در پاسخ گذرواژه برای رمزنگاری برگردانده می‌شود.

شناسه‌ی قربانی همراه با اطلاعات وضعیتی (فرآیند رمزنگاری انجام شده یا نه) در بخش رجیستری ذخیره می‌شود. باج‌افزار پرونده‌ها با پسوندهای مشخص را در درایوها جستجو کرده و با استفاده از AES آن‌ها را رمزنگاری می‌کند. این باج‌افزار پسوند مشخصی را به پرونده‌های رمزنگاری شده اضافه می‌کند که این پسوند رشته‌ی «HL~.» است که در ادامه‌ی آن نیز 5 حرف از گذرواژه‌ی رمزنگاری می‌آید.

Hades Locker پرونده‌های متنوعی را هدف گرفته است اما از پرونده‌هایی که در مسیر آن‌ها رشته‌های زیر وجود دارد، صرفنظر می‌کند:

windows, program files, program files (x86), system volume information و $recycle.bin.

این باج‌افزار همچنین رونوشت‌های Shadow Volume را حذف می‌کند تا قربانی از طریق آن‌ها نتواند پرونده‌های خود را بازیابی کند.

پیغام باج‌خواهی که در کامپیوتر قربانی نمایش داده می‌شود، پیوندهایی به وب‌گاه‌های

n7457xrhg5kibr2c.onion http://pfmydcsjib(dot)ru http://jdybchotfn(dot)ru

دارد که کاربر را تشویق می‌کند تا از این وب‌گاه‌ها برای آگاهی از مقدار باج و نحوه‌ی پرداخت آن، دیدن کنند. هنگامی که قربانی به این وب‌گاه‌ها متصل می‌شود،

در ایـن وب‌گاه‌هـا اطلاعاتـی در مـورد مقـدار بـاج و آدرس بیت‌کویـن کـه بایـد بـاج را پرداخـت کننـد و نحـوه‌ی بدسـت آوردن بیت‌کویـت ارائـه شـده اسـت. ایـن وب‌گاه ظاهـراً بـه شرکـت Hades تعلـق دارد و از چندیـن صفحـه تشـکیل شـده اسـت مثـل صفحـات سـؤالات متـداول، تسـت رمزگشـایی، بخـش کمک‌رسـانی و آمـوزش رمزگشـایی.

اخبار تحلیلی

سوءاستفاده‌ی بدافزارها از بستر عیب‌یابی ویندوز برای آلوده کردن کاربران

بستر عیب‌یابی ویندوز (WTP) در فهرست انتخابی سرویس‌های قانونی ویندوز قرار گرفته که برای آلوده کردن کامپیوتر کاربران به بدافزار مورد سوءاستفاده قرار می‌گیرد.

براساس تحقیقات محققان Proofpoint این تکنیک آخر در داخل اسناد ورد و در پرونده‌های ضمیمه هرزنامه‌ها مورد استفاده قرار گرفته است.

هنگامی که کاربر سند ورد را باز می‌کند، با انبوهی از نویسه‌های درهم و برهم و یک هشدار در بالای سند مواجه می‌شود. این پیام اعلام می‌کند: «این سند دارای کدگذاری اشتباه UTF8 است. دوبار کلیک کنید تا به‌طور خودکار مجموعه نویسه‌ها تشخیص داده شود.»

این هشدار چیزی بیش از یک شیء OLE نیست. یک عنصر تعاملی که می‌تواند در هر جایی از یک سند آفیس تعبیه شود.

برخی کاربران شرطی شده‌اند که از عیب‌یابی ویندوز استفاده کنند.

محققان Proofpoint اعلام می‌کنند، کلیک بر روی این پیغام، اجرای یک پرونده‌ی DIAGCAB را آغاز می‌کند. DIAGCAB یک فرمت پرونده است که به بستر عیب‌یابی ویندوز ضمیمه شده است، سامانه‌ای که توسط مایکروسافت ایجاد شده تا به شرکت‌ها و OEM اجازه می‌دهد تا اجرای فرآیند عیب‌یابی و تعمیر را خودکار نماید.

تمامی کاربران زمانی که در اتصال به اینترنت آن‌ها مشکلی وجود داشته باشد، این پنجره‌ی عیب‌یابی را مشاهده و روی آن کلیک کرده‌اند. برخی اوقات این فرآیند تنظیمات ارتباط با اینترنت را تعمیر کرده است و از این رو بسیاری از کاربران شرطی شده‌اند تا هر زمان که پنجره‌ی عیب‌یابی را مشاهده می‌کنند روی گزینه‌ی «بعدی» کلیک کنند.

اجرای اسکریپت PowerShell با استفاده از پرونده‌های DIAGCAB

در مورد پویش اخیر هرزنامه‌ای، کلیک دوباره بر روی این پیغام هشدار، برای تشخیص مجموعه نویسه‌های سند، یک پنجره‌ی عیب‌یابی را اجرا می‌کند که چیزی بیش از یک پرونده‌ی DIAGCAB نیست. این پرونده حاوی اسکریپت‌های خودکار PowerShell است که بنا به گزارش Proofpoint، تروجان درب پشتی LatentBot را بارگیری و نصب می‌کند.

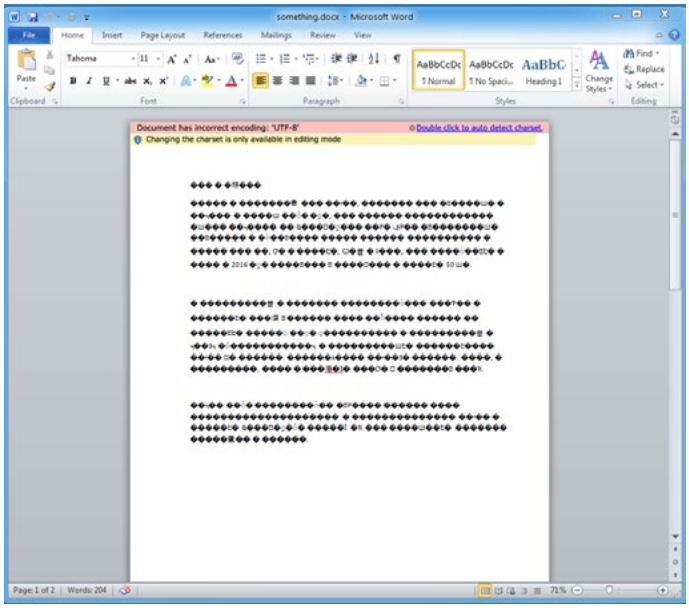
از دیدگاه فنی، تفاوتی بین اسکریپت‌های ماکرو و این اسکریپت‌های عیب‌یابی وجود ندارد، چرا که هر دو به مهاجم اجازه‌ی اجرای یک سری عملیات خودکار را می‌دهند.

تنها تفاوت این است که ابزارهای امنیتی، اسکریپت‌های

ماکـرو را بـرای بدافزارهـا بررسـی می‌کننـد درحالی‌کـه از بررسـی اسـکریپت‌های عیب‌یابـی صرفنظـر می‌شـود.

عـلاوه بـر بسـتر عیب‌یابـی ویـنـدوز، قبـلاً نویسـندگان بدافـزار از سـایر سرویس‌هـا و ویژگی‌هـای ویـنـدوز همچـون ابـزار مدیریـت ویـنـدوز (WMI)، قابلیـت همـکاری آفیـس، سرویـس انتقـال هوشـمند پس‌زمینـه و زمانبنـد وظیفـه سوءاسـتفاده کرده‌انـد.

خوشـبختانه ایـن تکنیـک شـبیه بـه اسـکریپت‌های ماکـرو نیـاز بـه تعامـل کاربـر دارد، بنابرایـن کاربرانـی کـه بـا مفاهیـم امنیتـی آشـنا باشـند، متوجـه خواهنـد شـد کـه ایـن یـک پیغـام و هشـدار خطرنـاک اسـت و مدیـر سـامانه را بـرای بررسـی‌های بیشـتر در جریـان خواهنـد گذاشـت.



اخبار تحلیلی

مبهم‌سازی: بهترین دوست بدافزارها (بخش ۱)

هر روزه شاهد بدافزارهای مختلفی هستیم. این بدافزارها شامل باتنت‌هایی هستند که می‌خواهند یک کارگزار را هدف قرار دهند یا باج‌افزار هستند که پرونده‌های شما را رمزنگاری کرده و از شما باج می‌خواهند. همه‌ی این بدافزارها می‌خواهند در طول فرآیند آلوده‌سازی و انجام عملیات خود، مخفی باقی بمانند تا حذف نشده و مورد تحلیل قرار نگیرند.

بدافزارها با استفاده از تکنیک‌های مختلفی برای در امان ماندن از تشخیص و تحلیل، به این هدف می‌رسند. برخی از این تکنیک‌ها شامل نامفهوم کردن نام پرونده، تغییر ویژگی‌های پرونده‌ها یا انجام فعالیت تحت یک برنامه یا سرویس قانونی است. در برخی نمونه‌های پیچیده ممکن است بدافزار تلاش کند، برنامه‌های تشخیص مدرن را براندازد تا از تشخیص داده شدن و اینکه چه فرآیندها و ارتباطاتی را اجرا می‌کند، جلوگیری نماید.

با وجود پیشرفت‌های زیاد در عرصه‌ی بدافزارها، برنامه‌های بد تا همیشه نمی‌توانند مخفی باقی بمانند. زمانی که بدافزار پیدا شد، به لایه‌های دفاعی بیشتری نیاز دارد تا از تحلیل و مهندسی معکوس در امان باشد.

با پیاده‌سازی سازوکارهای دفاعی بیشتر، تشخیص و از کار انداختن بدافزار بسیار سخت خواهد بود. هرچند تکنیک‌های مختلفی برای مخفی کردن داخلی بدافزار استفاده می‌شود، روشی که امروزه توسط هر بدافزاری استفاده می‌شود، مبهم‌سازی بایزی است.

مبهم‌سازی (در زمینه نرم‌افزار) یک تکنیک است که باعث می‌شود بایزی و داده‌های متنی قابل خواندن نباشند یا سخت درک شوند. توسعه‌دهندگان نرم‌افزار گاهی اوقات از تکنیک مبهم‌سازی استفاده می‌کنند چرا که آن‌ها نمی‌خواهند برنامه‌های آن‌ها مهندسی معکوس شده یا به سرقت برود.

پیاده‌سازی مبهم‌سازی می‌تواند به سادگی تغییر دادن چند بیت و یا به پیچیدگی استفاده از رمزنگاری‌های استاندارد (همچون AES، DES و غیره) باشد. در اصطلاح بدافزارها مخفی کردن تعداد کافی و مشخصی از کلمات مفید خواهد بود چرا که این رشته‌ها دیدی از رفتار بدافزار را به تحلیلگر ارائه می‌دهد. مثالی از این رشته‌ها می‌تواند آدرس‌های URL مخرب یا کلیدهای رجیستری باشد. گاهی بدافزارها پا را فراتر گذاشته و مبهم‌سازی را بر روی کل پرونده با برنامه‌های خاصی که packer نامیده می‌شوند، اعمال می‌کنند.

بیایید مثال‌های عملی از مبهم‌سازی که در بسیاری از بدافزارهای امروزی مورد استفاده قرار می‌گیرد را بررسی کنیم.

سناریوی اول: عملیات XOR

یکی از روش‌های معمول مبهم‌سازی استفاده از عملگر XOR ست. رایج بودن این روش به دلیل سادگی در

پیاده‌سازی و مخفی کردن پرونده‌ی بدافزار از چشم‌های غیرحرفه‌ای است. داده‌های پررنگ‌شده در تصویر زیر را بررسی کنید.

این داده‌های مبهم‌سازی شده در حالت فعلی قابل خواندن نیستند. اما زمانی که عملگر XOR با مقدار 0x55 اعمال می‌شود، کلا چیز دیگری مشاهده می‌شود.

اعمال عملگر XOR با مقدار 0x55، آدرس URL مخرب را نشان می‌دهد. حال URL مخرب را در دست داریم. به نظر می‌رسد این بدافزار به آدرس http://tator1157.hostgator.com متصل می‌شود تا پرونده‌ی bot.exe را بازیابی کند.

این شکل از مبهم‌سازی به‌طور معمول برای شکستن بسیار آسان است. حتی اگر کلید XOR را نداشته باشید، برنامه‌هایی وجود دارد که در پرس‌وجوی یک رشته‌ی مشخص، هر مقدار تک‌بایتی XOR را در چرخه‌ای به‌طور دستی انجام دهد. یک ابزار در دسترس برای بستر یونیکس و ویندوز XORSearch است که توسط دیدیر استیونس نوشته شده است.

از آنجایی که نویسندگان بدافزار می‌دانند که چنین ابزاری وجود دارد، از تکنیک‌های مخصوص خود برای جلوگیری از تشخیص استفاده می‌کنند. یکی از کارهایی که ممکن است انجام دهند استفاده از چرخه‌ی دوتایی است و یا اجرای XOR بر روی داده با استفاده از یک مقدار مشخص و در دور دوم اجرا با مقدار دیگر است. یک تکنیک ویژه (هرچند مؤثر) که به‌طور معمول استفاده می‌شود، افزایش مقدار XOR داخل یک حلقه است. با توجه به تکنیک آخر می‌توان بر روی حرف n با 0x55 و در ادامه حرف t با 0x56 عملیات XOR انجام داد و این روند را تا آخر پیش گرفت. این تکنیک نیز می‌تواند توسط برنامه‌های XOR معمول، شکسته شود.

در ادامه و در پستی دیگر، سایر مثال‌های عملی از مبهم‌سازی ارائه خواهد شد.

اخبار تحلیلی

باج‌افزار DXXD حتی پرونده‌های شبکه‌های اشتراکی نگاشت‌نشده را نیز رمزنگاری می‌کند

خانواده‌ی جدیدی از باج‌افزارها پدیدار شده که کارگزارها را هدف قرار داده و پرونده‌ها بر روی شبکه‌ی اشتراکی را حتی اگر با کامپیوتر آلوده، نگاشت نشده باشد نیز رمزنگاری می‌کند.

این باج‌افزار با نام DXXD به‌عنوان نمونه‌ی جدید باج‌افزاری، پس از نمایش پیغام باج در کامپیوتر آلوده، پسوند .dxxd را به پرونده‌های رمزنگاری‌شده اضافه می‌کند. این بدافزار تنها در جستجوی پرونده‌های ماشین آلوده برای رمزنگاری نبوده و شبکه‌های اشتراکی نگاشت‌شده و نگاشت‌نشده را هدف قرار می‌دهد، ویژگی که قبلاً در باج‌افزار Locky دیده شده است. لارنس آبرامز از انجمن BleepingComputer اشاره می‌کند هرچند که در حال حاضر بردار آلودگی این باج‌افزار مشخص نیست، ولی این باور وجود دارد که مهاجمان سرویس رومیزی راه دور را مورد بهره‌برداری قرار داده و برای گسترش این باج‌افزار از جستجوی فراگیر بر روی گذرواژه‌ها استفاده می‌کنند.

این تهدید جدید در پیغام باج‌خواهی از کاربران می‌خواهد که با عوامل این باج‌افزار از طریق دو آدرس رایانامه در ارتباط باشند تا آموزش‌های مربوط به پرداخت را به قربانیان بدهند. این آدرس‌های رایانامه عبارتند از rep_stosd[at]protonmail.com و rep_stosd[at] tuta.io. هرچند که در اغلب آلودگی به باج‌افزارها توصیه می‌شود که قربانیان به این مسئله توجه نکرده و باج را پرداخت نکنند.

برخلاف سایر باج‌افزارهایی که تاکنون دیده شده، DXXD طوری پیکربندی شده تا تنظیمات رجیستری را تغییر می‌دهد تا زمانی که کاربر به سامانه وارد می‌شود، یک اطلاعیه‌ی قانونی را نمایش دهد. بخاطر همین، نویسندگان باج‌افزار مطمئن هستند زمانی که کاربر وارد سامانه‌ی آلوده می‌شود، پیغام باج به کاربر نمایش داده خواهد شد.

این اطلاعیه‌ی قانونی به کاربر اعلام می‌کند، سامانه‌ای که شما وارد آن شدید، توسط مهاجمان آلوده شده است. همچنین ادعا می‌کند که کاربران برای دریافت اطلاعات بیشتر و توصیه‌ها باید با متخصصان از طریق رایانامه‌های ذکر شده و همچنین آدرس‌های shellexec[at]protonmail.com یا null_ptr[at]tutanota.de در ارتباط باشند.

برای نمایش این اطلاعیه مهاجمان کلید رجیستری

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption

را تغییر می‌دهند. همچنین کلید

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText

را تغییر می‌دهند تا پیام زیر را نمایش دهد: «زمانی که شما کار با ویندوز را آغاز می‌کنید، محافظ ویندوز کار می‌کند تا با پویش پرونده‌ها مخرب و برنامه‌های

ناخواسته از کامپیوتر شما حفاظت کند.»

باتوجه به گفته‌های آبرامز، نویسنده‌ی باج‌افزار تصمیم گرفته که قربانیان و محققان را با ایجاد یک حساب کاربری در BleepingComputer دست بیندازد. او در این انجمن اعلام کرده نسخه‌ی جدیدی از باج‌افزار توسعه داده شده که رمزگشایی آن نیز بسیار سخت است. این توسعه‌دهنده‌ی بدافزار همچننی مدعی شده که از یک آسیب‌پذیری روز-صفرم برای آلوده کردن کامپیوترها و نصب باج‌افزار استفاده شده است.

محققان می‌گویند در مواجه با رخدادن آلودگی به باج‌افزار، پرداختن باج راه‌حل مناسبی نیست چرا که تضمین نمی‌کند داده‌های شما بازیابی شود. برای اینکه داده‌ها امن باقی بمانند، توصیه می‌شود که کاربران

- به‌طور مستمر از داده‌ها پرونده‌های پشتیبان تهیه کنند
- نرم‌افزارهای خود را به‌روز نگه دارند
- از یک راه‌حل ضدبدافزاری شناخته‌شده استفاده کنند
- از باز کردن ضمیمه‌ها با کلیک بر روی پیوندهای رایانامه‌های ناشناس خودداری کنند
- پروتکل رومیزی راه دور (RDP) و پرونده‌هایی که از پوشه‌ی AppData/LocalAppData در حال اجرا شدن هستند را غیرفعال کنند.

اخبار تحلیلی

کارگزارهای کنار گذاشته شده‌ی C&C موبایل، فرصتی حی و حاضر برای مهاجمان

زمانی که برنامه‌نویسان برنامه‌های کاربردی موبایل را می‌نویسند، تنها کدهای مربوط به عملکرد برنامه را در آن نمی‌گنجانند، بلکه کیت‌های توسعه‌داده شده‌ی برنامه‌های شخص ثالث برای تبلیغات، تجزیه و تحلیل و کارهای دیگری را نیز در کدهای خود جای می‌دهند. بزرگ‌ترین عملکرد SDK ها برقراری ارتباط با یک کارگزار مرکزی و دریافت دستورات و محتوا است اما محققان دریافتند که بسیاری از این کارگزارها کنار گذاشته شده‌اند و نمونه‌های سالمی از آن‌ها برای ثبت‌نام و برای خرید در شرکت GoDaddy مورد استفاده قرار گرفته‌اند.

این یک فرصت بزرگ برای مهاجمان است تا کدهای مخرب خود را بر روی این کارگزارها قرار داده و به دستگاه‌های اندروید و iOS آسیب بزنند.

ژی خو در کنفرانس بین المللی بولتن ویروس گفت: «صدها نمونه از این شرکت‌های استارتاپ SDK در یک دوره راه‌اندازی شدند. اما بسیاری از این استارتاپ‌ها از بین رفتند و کسی از این زیرساخت‌ها نگهداری نکرد. بخش بزرگی از این زیرساخت در حال حاضر نگهداری نمی‌شود. اگر این زیرساخت نگهداری نشود، برنامه‌های دارای این SDK ها تلاش خواهند کرد با کارگزار مرکزی خود ارتباط برقرار کرده و دستورات و محتوا را دریافت کنند ولی هیچ پاسخی دریافت نخواهند کرد. به محض اینکه این دامنه‌ها منقضی شوند، مهاجم می‌تواند این دامنه‌ها و زیرساخت را در دست گرفته و دستورات و محتوای مخرب ارسال کند.»

محققان مقاله با نام «مواظب باشید! زامبی‌ها می‌آیند.» چاپ کرده‌اند که نه تنها خطرات را توضیح می‌دهد، بلکه کمیت تعداد دامنه زامبی‌های رها شده را نیز برآورد می‌کند.

خو گفت محققان 2.8 میلیون نمونه برنامه‌ی APK را بررسی کرده‌اند که از 575 هزار دامنه‌ی ریشه‌ی منحصربفرد استفاده می‌کنند. البته 65 هزار نمونه از آن‌ها پاسخی نمی‌دهند و به‌عنوان زامبی در نظر گرفته شده‌اند و 33 هزار نمونه نیز توسط GoDaddy قابل دسترس هستند.

محققان همچنین رفتار مشتریان قانونی و مخرب را در استفاده آن‌ها از پروتکل‌های از پیش تعریف‌شده در ارتباط با یک کارگزار اصلی، مورد مطالعه قرار دادند. آن‌ها متوجه شدند که هر دو دسته رفتار مشابهی را نشان می‌دهند و علاقه به استفاده از سرویس‌هایی همچون مدیر تلفن، سرویس‌های مکان‌یابی، پیام کوتاه و مدیریت حساب دارند.

خو گفت: «این مسئله فقط بستگی به این دارد که دامنه‌ی اصلی را چه کسی کنترل می‌کند و تصمیم می‌گیرد که چه کار خوب یا بدی را انجام دهد.»

محققان گفتند هنگامی که یک مهاجم اقدام به خرید و کنترل یک دامنه زامبی نماید، می‌تواند دوباره کانال

ارتباطی اصلی را اجرا کرده و امتیازات همان مدیریت قبلی را بدست آورد. به‌عنوان مثال کتابخانه‌های تبلیغات تهاجمی، می‌توانند شروع به جمع‌آوری اطلاعات مکانی در کنار اطلاعاتی که از وسیله‌ی قربانی همچون نوع و اطلاعات IMSI بدست می‌آورد بکند تا تبلیغات را به شماره‌ی درستی ارسال کند. مهاجم همچنین می‌تواند به‌طور خودکار از طریق این کانال، برنامه یا کد مخرب را به شماره‌ی کاربر ارسال کند. مهاجم می‌تواند قابلیت جاوا اسکریپت را در Webview فعال کند تا تبلیغات به‌طور خودکار نمایش داده شده و همچنین بتواند قابلیت اجرای کد از راه دور را داشته باشد.

محقق دیگری با نام لو بیان کرد: «دامنه‌هایی که برنامه‌های کاربردی HTML5 را کنترل می‌کنند، به‌طور بالقوه در معرض خطر بیشتری هستند چرا که این برنامه‌ها از طریق کانال، تزریق و اجرای برنامه‌های جاوا اسکریپت را نیز پشتیبانی می‌کنند. همچنین در این برنامه‌ها امکان بهره‌برداری از میان‌افزارهایی همچون PhoneGap و RhoMobile که از محتوای وب غنی‌تری پشتیبانی می‌کنند، وجود دارد.»

لو ادامه داد: «به‌عنوان مثال PhoneGap افزونه‌هایی را نصب می‌کند که از انتقال پرونده، واسط رایانامه و پیامک، قابلیت اجرای کد از طریق دستورات شِل و ویژگی‌های LaunchMyApp پشتیبانی می‌کند.»

پژوهشگران توضیح دادند که یک برنامه مانند RogueSports است که هنوز هم از طریق Google Play و App Store و از طریق بازار تلفن ویندوز در دسترس است و از سال 2014 به‌روزرسانی نشده است و از طریق GoDaddy به قیمت 12 دلار به فروش می‌رسد. مهاجمان می‌توانند کدهای مخرب نوشته شده در جاوا اسکریپت را تزریق کنند که می‌تواند بر روی دستگاه اجرا شود و به مهاجم اجازه خواهد داد یک iframe جاسازی کرده، مدارک و داده‌های دیگر را به سرقت ببرد و یا بدافزار را راه‌اندازی کنند.

خو گفت: « این مهم است که درک کنید که یک SDK قانونی و زیرساخت های دستور و کنترل آن می‌تواند خطرناک باشد. قبل از اینکه مجوزها را به یک برنامه بدهید، تمام مؤلفه‌های آن را در بخش تشخیص بدافزار برای دیدن SDK ها بررسی کنید که تا زیرساخت دستور و کنترل آن بدون مدیریت باقی نمانده باشد.»

اخبار تحلیلی

استفاده از پرس‌وجوهای WMI توسط بدافزارها برای فرار از تشخیص

به گفته‌ی محققان FireEye، بدافزارها روز به روز بیشتر از پرس‌وجوهای ابزار مدیریت ویندوز (WMI) برای فرار از تشخیص و همچنین برای تشخیص محیطی که در حال اجرا بر روی آن هستند، استفاده می‌کنند.

بهره برداری از WMI برای فرار از تشخیص قبلاً نیز مشاهده شده است و Mandiant نیز سال گذشته کشف کرد که گروه‌های تهدیدات مداوم پیشرفته (APT) از WMI و PowerShell برای حرکت جانبی، برداشت اعتبار و جستجوی اطلاعات مفید در محیط ویندوز استفاده می‌کنند. و اینک FireEye مثال‌های ویژه‌ای را ارائه کرده که پرس‌وجوهای WMI برای مقاصد نابکار مورد استفاده قرار می‌گیرد.

از آن‌جایی که WMI تعامل سطح بالایی را با اشیای ویندوز از طریق Jscript، VBScript، C/C++ و #C ایجاد می‌کند، سرویس‌های WMI توسط نویسندگان بدافزار برای فرار از تشخیص و تشخیص محیط مجازی مورد بهره‌برداری قرار می‌گیرد. در واقع FireEye توضیح می‌دهد پرس‌وجوی WMI می‌تواند برنامه‌های ضدویروس را تشخیص دهد بخاطر اینکه آن‌ها در کلاس AntiVirusProduct تحت فضای نام root\SecurityCenter2 ثبت شده‌اند.

برخی از بدافزارها در وهله‌ی اول نوع سامانه‌ی عامل را بررسی می‌کنند و اگر سامانه عامل ویندوز ویستا یا نسخه‌های قبلی باشد، به دنبال برنامه‌ی ضدویروس خواهد گشت. به محض اینکه بدافزار نوع سامانه‌ی عامل و ضدویروس را تشخیص داد، اطلاعات و سایر داده‌های کاربر را برای کارگزار خود ارسال می‌کند تا بار داده‌ی مناسب را دریافت کرده و یا از تشخیص بگریزد.

بنابه گفته‌ی FireEye، برخی بدافزارها سامانه را با تکنیک‌های مختلف و پرس‌وجوهای WMI، برای چند محصول امنیتی و برنامه‌های معروف مجازی‌سازی بررسی می‌کند. بدافزار اطلاعات BIOS را در کلاس Win32_BIOS و تحت فضای نام root\cimv2 بررسی می‌کند. FireEye می‌گوید: «هر فیلد/ستون شبیه به پرس‌وجوهای SQL قابل بازیابی است.»

محققان امنیتی همچنین برخی نمونه‌ها را پیدا کردند که از کلاس Win32_ComputerSystem برای تشخیص محیط مجازی استفاده می‌کند که در نتیجه مدل آن برنامه‌ی مجازی‌سازی را برمی‌گرداند و اطلاعاتی مانند ماشین مجازی VirtualBox، Vmware و Virtual Machine را ارائه می‌کند. اگر رشته‌ی انطباقی پیدا شود، مجازی‌سازی تشخیص داده می‌شود.

برخی دیگر از بدافزارها در کنار نام فرآیندهای

VMware، Wireshark، Fiddler و سایر محصولات امنیتی، قبل از پرس‌وجوهای WMI، از کلاس‌های Win32_VideoController و Win32_DiskDrive برای تشخیص استفاده می‌کنند. زمانی که پرس‌وجوی WMI در PowerShell اجرا شود مقدار زیادی از اطلاعات مربوط به Vmware را نشان می‌دهد.

خانواده‌ی بدافزاری دیگری مشاهده شده که از کلاس Win32_DiskDrive، برای تشخیص VirtualBox، Virtual Hard دیسک و VMware استفاده می‌کند. محققان امنیتی اشاره کردند: «هر زمان که یکی از این ماشین‌های مجازی تشخیص داده شود، این فرآیند خاتمه می‌یابد و از تحلیل رفتاری بدافزار جلوگیری به عمل می‌آید.»

همچنین مشاهده شده که بدافزار تنها به دنبال بررسی فرآیندی خاص در کلاس Win32_Process نبوده و بلکه آن فرآیند را می‌کُشد. یک برنامه‌ی کاربردی که توسط کد مخرب هدف قرار گرفته است، اشکال‌یاب شناخته‌شده‌ی Immunity است که بنا به گفته‌ی FireEye «خاتمه یافته و پس از تغییر مجوزها با استفاده از شِل میزبان اسکریپت ویندوز، پوشه‌های آن حذف شده است.»

همچنین برخی بدافزارها قصد جستجو و خاتمه دادن به فرآیندهای ضدویروس شرکت Kingsoft را دارند. برای پیدا کردن یک فرآیند، یک بدافزار معمولا از واسط‌های برنامه‌نویسی

(API) CreateToolHelp32Snapshot, Process32First , Process32Next

استفاده می‌کند، اما نویسندگان بدافزار تصمیم به استفاده از پرس‌وجوهای WMI گرفتند که امکان جابجایی با ده‌ها خط کد را می‌دهد.

دیده شده که یک تولیدکننده‌ی کلید مایکروسافت آفیس، سرویس حفاظت از نرم‌افزار آفیس ویندوز را با استفاده از پرس‌وجوهای WMI بررسی می‌کند. اگر این سرویس در حال اجرا نباشد، بدافزار آن را شروع کرده و به شیء سرویس حفاظت از نرم‌افزار آفیس ویندوز دسترسی یافته و سپس کلید محصول آفیس را نصب خواهد کرد.

FireEye می‌گوید: «نویسندگان بدافزار همواره به دنبال روشی برای گریز از چارچوب‌های تحلیلی و جعبه شنی هستند تا اجرای بار داده را با موفقیت در محیط و بستر هدف انجام دهند. WMI روش ساده‌ای را برای تشخیص محیط ارائه می‌کند که می‌تواند برای گریز از محیط‌های تحلیل پویا و جعبه شنی مورد استفاده قرار گیرد که به نظر می‌رود این روش ساده در مهندسی معکوس و سایر انجمن‌های امنیتی دستِ کم گرفته شده است. گام‌های کاهشی برای نظارت بر پرس‌وجوهای WMI که برای فرار از تشخیص استفاده می‌شود، باید اتخاذ شود.»

اخبار تحلیلی

تبانیِ برنامه‌های موبایل، سازوکارهای معمول امنیتی را دور می‌زنند!

سازوکارهای معمول دستگاه‌های اندروید همچون جعبه شنی، در برابر تهدیدهای مربوط به یک برنامه در آنِ واحد حفاظت می‌کنند ولی اگر چند برنامه با هم تبانی کنند، می‌توانند این سازوکارهای معمول را دور بزنند.

روز چهارشنبه در 26مین کنفرانس بین‌المللی بولتن ویروس، محققان این تهدید را از حالت تئوری به عملی تبدیل کردند. آن‌ها چند برنامه با نسخه‌های آلوده از MoPlus SDK را عرضه کردند که در کنسرت‌ها اجرا شده و هزینه‌ی پیامک‌ها را شارژ کرده و اطلاعات شخصی ذخیره‌شده را به سرقت می‌برد و حتی اجرای بار داده را هم‌گام‌سازی می‌کنند.

در یک سخنرانی با عنوان «تبانی اندرویدهای وحشی»، جورجه بلاسکو از دانشگاه شهر لندن، گفت **که برنامه‌های تلفن همراه اغلب برای تبادل اطلاعات بی‌خطر با یکدیگر در ارتباط هستند. اما این روند می‌تواند توسط یک مهاجم که یک برنامه با مجوزهای بالایی دارد بهم بخورد و از این طریق اطلاعات مهم و حساس را از دستگاه قربانی بدست آورده و از طریق اینترنت به برنامه‌ی دیگری ارسال کند. به‌عنوان مثال، می‌تواند این اطلاعات را به کارگزار مهاجم ارسال کند درحالی‌که کاربری در ناآگاهی به سر می‌برد.**

بلاسکو گفت: «کاربر اطلاعی از ارتباط میان برنامه‌ها ندارد و نمی‌تواند تصمیمی آگاهانه برای اعطای مجوزها به برنامه‌ها بگیرد.»

مقاله‌ای که بلاسکو و همکارانش در این کنفرانس ارائه دادند، شرح می‌دهد که چگونه ارتباطات بین برنامه‌ای به‌طور مثال در اندروید، می‌تواند محدودیت‌های جعبه شنی را دور بزند. در اندروید این ارتباط از طریق intent همه‌پخشی حاصل می‌شود و پیامی است که عملیاتی که باید انجام شود را توضیح می‌دهد. مهاجمان می‌توانند برنامه‌ها با دسترسی‌های مختلف را مجبور کنند تا داده‌های حساس را از طریق اینترنت به سایر برنامه‌ها ارسال کنند.

محققان نوشتند: «تشخیص این تبانی بین برنامه‌ها بسیار سخت است چرا که هر برنامه سعی می‌کند خود را به‌عنوان ابزاری بی‌خطر نشان دهد. این تکنیک تبانی، مهاجم را قادر می‌سازد تا به دستگاه‌های بیشتری برای بازه‌ی زمانی طولانی‌تر نفوذ کند قبل از اینکه به دام بیفتد.»

بلاسکو در طول سخنرانی خود توضیح داد که این برنامه‌های تبانی‌کننده می‌توانند از کانال‌های بیشتری به علاوه‌ی intent هایی که برای کار با هم نیاز دارند، استفاده کنند. یکی از این کانال‌ها نگه‌دارنده‌ی محتوا در قالب جدول‌هایی خواهد بود که به سایر برنامه‌ها امکان خواندن، به‌روزرسانی و ایجاد جدول و اطلاعات مهم را خواهد داد. ذخیره‌ساز خارجی، کانال دیگری در اندروید است که تمام برنامه‌ها به بخش‌های مختلف آن دسترسی

دارند و به کاربرانی که مجوز نوشتن دارند، اجازه‌ی نوستن و خواندن از این حافظه‌ی خارجی را می‌دهد. این حافظه‌ی خارجی می‌تواند به‌عنوان یک دراپ‌باکس مشترک بین برنامه‌های تبانی‌کننده مورد استفاده قرار بگیرد.

بلاسکو می‌گوید، تنظیمات اشتراکی یک کانال کلیدی برای تبانی است. برنامه‌ها جفتِ کلید-مقدار داده‌ها مخصوصاً داده‌های پیکربندی برنامه‌ها و تنظیمات مشترک را در تنظیمات اشتراکی ذخیره می‌کنند. در نسخه‌های قبل‌تر از اندروید 4.4 که SELinux برای سامانه عامل معرفی شد، تنظیمات اشتراکی می‌تواند توسط برنامه‌ها برای برقراری ارتباط مورد استفاده قرار گیرد.

بلاسکو گفت محققان تنظیمات اشتراکی را به‌عنوان نقطه‌ی شروعی برای پیدا کردن تبانی بین برنامه‌ها در نظر می‌گیرند. با استفاده از مجموعه داده‌ی فراهم‌شده توسط Intel Security، 50 هزار برنامه مورد بررسی قرار گرفت و محققان دریافتند که برنامه‌ها برای تبادل داده از حافظه‌ی اشتراکی استفاده می‌کنند تا اجرای بار داده در MoPlus SDK را هم‌گام‌سازی کنند.

برنامه‌ی MoPlus به‌عنوان یک دربِ پشتی بالقوه در ماه نوامبر 2015 کنار گذاشته شد ولی تبانی بین برنامه هم‌اکنون کشف شده است.

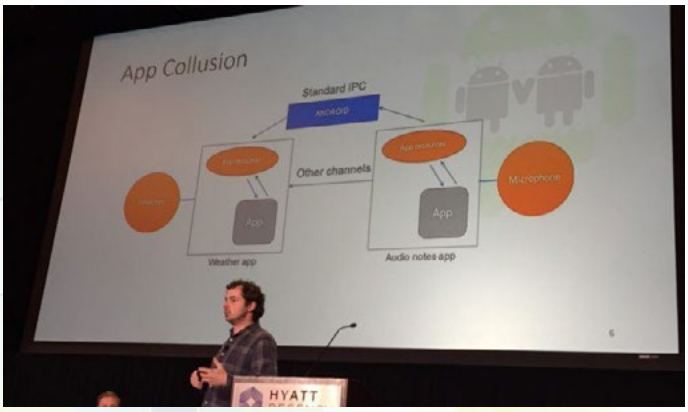
بلاسکو گفت برنامه‌هایی که از MoPlus SDK استفاده می‌کنند، می‌توانند با هم ارتباط داشته باشند و بفهمند که بالاترین سطح دسترسی متعلق به کدام برنامه است. او با یک مثال این مسئله را نشان داد که 3 برنامه وجود داشت. برنامه‌ای که بالاترین سطح دسترسی و امتیازات را داشت می‌توانست یک کارگزار HTTP را باز کند و دستورات و محتوا را از کارگزار مهاجم دریافت کند.

بلاسکو گفت: «MoPlus SDK که بر روی برنامه‌های مختلف در حال اجراست، از تنظیمات اشتراکی به‌عنوان کانال ارتباطی استفاده می‌کند که یک رهبر برای ارتباط با کارگزار دستور و کنترل انتخاب خواهد کرد. برنامه‌ها با هم تعامل خواهند داشت تا بدانند کدام‌یک بیشترین دسترسی را دارد و به‌عنوان نماینده با کارگزار دستور و کنترل ارتباط برقرار کرده و دستورات را دریافت می‌کند. آن‌ها می‌توانند حمله را بهینه کرده و تنها از برنامه‌ای که بیشترین دسترسی به سامانه دارد را استفاده کنند.»

بلاسکو بیان کرد، محققان تنها این نوع از حملات هم‌گام‌سازی را پیدا کردند ولی هیچ حمله‌ی سرقت اطلاعات در دنیای واقعی یافت نشد.

برای انجام اقدامات متقابل، بلاسکو گفت باید روش‌هایی برای تشخیص تبانی بین برنامه‌ها توسعه داده شود و گوگل نیز محدودیت‌هایی بر روی ارتباطات بین برنامه‌ها اعمال کند. در عین حال، نویسندگان و توسعه‌دهندگان برنامه‌های موبایل باید قبل از گنجاندن کدهای شخص ثالث در برنامه‌های خود، آن‌ها را تحلیل کنند.

بلاسکو در ادامه افزود: «ارتباطات مختلف بین برنامه‌های موبایل، ریسک و تهدیدهای جدیدی را معرفی می‌کند. تبانی بین برنامه‌ها ممکن است چرا که کاربر هیچ اطلاعی از ارتباط بین برنامه‌ها ندارد. کاربران باید مراقب مجوزهایی که به برنامه‌ها اعطا می‌کنند باشند نه اینکه به ارتباطات و داده‌هایی که برنامه‌ها با هم به اشتراک می‌گذارند، توجه کنند.»



اخبار تحلیلی

شکستن تکنولوژی JEA مایکروسافت برای نفوذ به سامانه‌ها

محقق امنیتی مت ویکس راهی را کشف کرده که از تکنولوژی JEA مایکروسافت برای ارتقاء پروفایل کاربران سوءاستفاده می‌کند.

JEA یک تکنولوژی در مایکروسافت است که قابلیت تفویض مدیریت برای اجرای وظایف از طریق PowerShell را ممکن می‌سازد.

با استفاده از JEA به‌طور مناسب می‌توان نقش‌ها را برای مدیران پیکربندی کرد تا آن‌ها بتوانند تمام دستورات برای انجام وظایف خود را اجرا کنند و به دستورات دیگری دسترسی نداشته باشند.

حال یک محقق امنیتی روشی کشف کرده که با استفاده از آن می‌توان از قابلیت PowerShell و JEA برای ارتقاء پروفایل کاربر در سطح مدیر و سرپرست سامانه سوءاستفاده کرد.

این متخصص امنیتی تحلیل جالبی ارائه داده که در آن توضیح می‌دهد تکنولوژی JEA هیچ مانعی در برابر مهاجم ندارد تا او بتواند پروفایل خود را به مدیر سامانه ارتقاء دهد.

در پست وبلاگی که این محقق ارسال کرده می‌خوانیم: «تمامی پروفایل‌های JEA که مایکروسافت ارائه داده را مشاهده کردم که به راحتی برای دسترسی به حقوق مدیر سامانه قابل دور زدن است و این کار فوری، قابل اعتماد و بدون نیاز به پیکربندی خاصی انجام می‌شود. مدیران سامانه‌ای که پروفایل‌های مخصوص خود را ایجاد می‌کنند، خیلی کار خاص و بهتری انجام نمی‌دهند.»

این محقق روش‌های مختلفی را برای بهره‌برداری از تکنولوژی JEA ارائه کرده است. در راهنمای حمله‌ی JEA این محقق توضیح داده که چگونه با استفاده از Add-Computer- و دستور cmdlet می‌توان موانع JEA را شکست و امتیازات را ارتقاء داده و دسترسی و کنترل کامل بر روی یک سامانه‌ی نامحدود بدست آورد.

بسیار مهم است که اشاره شود این محقق از هیچ نقص روز-صفرم استفاده نکرده است. او ماشین را در دامنه‌ی جدیدی ایجاد/سوئیچ کرده و سپس قوانین گروه را از یک کنترل‌کننده‌ی دامنه تحت نظر مهاجم استخراج کرده و در نهایت پروفایل خود را با کنترل کامل بر سامانه ارتقاء می‌دهد.

این محقق می‌گوید: «کامپیوتر شما به دامنه اضافه خواهد شد. سپس ریبوت شده و قوانین گروه را از کارگزار جدید استخراج خواهد کرد. در نهایت پیکربندی قوانین گروه فعال خواهد شد. این پیکربندی‌ها باعث تغییر در برخی تنظیمات کامپیوتر شما مانند حذف شدن دیواره‌ی آتش، اجرای هر دستور اسکریپتی در شروع اولیه‌ی سامانه، زمان‌بندی وظیفه و ورود به‌عنوان مدیر سامانه خواهد شد. به عبارت دیگر موانع امنیتی شما شکسته شده و دسترسی نامحدود و کامل بر روی سامانه‌ی شما وجود

خواهد داشت.»

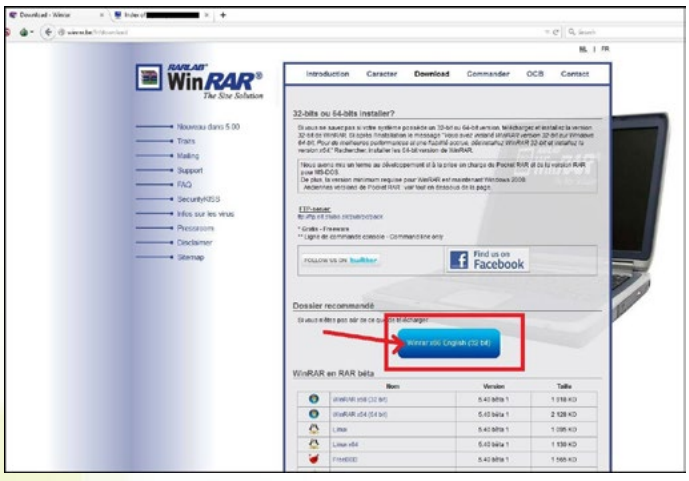
این محقق توضیح می‌دهد که مایکروسافت مخزن جامعی از پروفایل‌های JEA را مدیریت می‌کند. او یک مخزن مخفی در آدرس https://github.com/PowerShell/ JEA پیدا کرده است. در این مخزن قابلیت 4 نقش وجود دارد که عبارتند از: سطح 1 و سطح 2 برای سرپرست کارگزار عمومی و IIS ویژه‌ی سطح 1 و سطح 2.

این متخصص امنیتی می‌نویسد: «من از دستورات PowerShell زیر برای نصب IIS و ASP.NET استفاده کردم:

```
import-module servermanager
Install-WindowsFeature Web-Server
Install-WindowsFeature Web-ASP
»Install-WindowsFeature Web-Asp-Net45
```

یک مهاجم می‌تواند دستور New-Service cmdlet را اجرا کرده و هر دستوری را با دسترسی‌های SYSTEM اجرا کند. Cmdlet های Get-WinEvent و Get-EventLog به مهاجم اجازه می‌دهد دسترسی به رویدادهای ثبت‌شده‌ی ادمین را بدست آورد بدون اینکه عواقب آشکاری برای او وجود داشته باشد.

این محقق تاکید کرد که مایکروسافت مستند JEA را به‌روزرسانی کرده و جزئیات بیشتری در خصوص پروفایل‌های آن ارائه خواهد کرد و همچنین راهی برای مدیریت دسترسی‌های مدیریتی و سرپرستی پیشنهاد خواهد داد.



اخبار تحلیلی

سوءاستفاده‌ی بدافزار FastPOS از Mailslots ویندوز برای سرقت داده‌ها

عاملان بدافزار FastPOS تروجان خود را با یک سازوکار جدیدِ خروج داده به‌روزرسانی کرده‌اند که از سازوکار Mailslots ویندوز استفاده می‌کند تا داده‌ها را قبل از خروج از سامانه‌ی قربانی، ذخیره کند.

این نسخه‌ی جدید از بدافزار POS در ماه ژوئن مشاهده شد که محققان ترندمیکرو تبلیغات آن را در انجمن‌های زیرزمینی فروش کارت‌های به سرقت‌رفته کشف کردند.

FastPOS به‌روزرسانی خود را سالانه دریافت می‌کند!

تحلیل‌های انجام شده بر روی نسخه‌ی جدید خانواده بدافزارهای POS نشان می‌دهد که تمرکز این دسته بر روی سرعت و مخفیانه قربانی کردن است، برخلاف بدافزارهای POSی که تاکنون مشاهده شده است.

محققان ترندمیکرو پس از کشف اولیه این بدافزار و ردیابی ظهور این بدافزار به ماه مارس سال 2015، تحلیل‌های خود را ادامه دادند.

همچنین این محققان دریافتند که عاملان بدافزار FastPOS به‌روزرسانی این بدافزار را هر سپتامبر در فصل تعطیلات انجام می‌دهند. پس از گذشت ماه سپتامبر، اکنون ترندمیکرو جزئیات آخرین نسخه‌ی این بدافزار را منتشر کرده است.

FastPOS هم‌اکنون از نسخه‌ی 32 بیتی و 64 بیتی پشتیبانی می‌کند!

این شرکت امنیتی اعلام کرده که این بدافزار قابلیت آلوده کردن سامانه‌های 32 بیتی و 64 بیتی را دارد.

FastPOS که از دو ماژول اصلی (کی‌لاگر و اسکریپر حافظه) استفاده می‌کند، همچنین کارکرد خود در سطح فرآیندهای سامانه عامل را تغییر داده است. نسخه‌ی قبلی FastPOS در قالب یک فرآیند تودار کار می‌کرد در حالی‌که نشخه‌ی جدید ماژول اصلی و ثانویه آن هر یک در قالب یک فرآیند متفاوت سامانه عامل کار می‌کنند که حذف آن‌ها را سخت‌تر می‌کند.

در حقیقت ترندمیکرو می‌گوید تشخیص جریان‌های HTTP که از طریق آن بدافزار داده‌های کارت‌های اعتباری را از POS به سرقت برده است بسیار آسان است چرا که این اطلاعات رمزنگاری نشده است.

FastPOS اکنون از Mailslots ویندوز سوءاستفاده می‌کند!

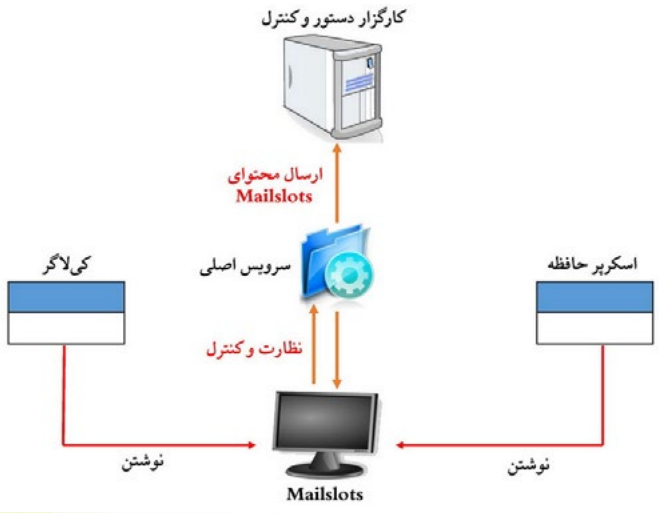
اما تغییر اساسی که در این بدافزار در نسخه‌ی جدید ایجاد شده مربوط به نحوه‌ی ذخیره‌سازی داده‌های به سرقت‌رفته پیش از ارسال به کارگزار دستور و کنترل است. درست مثل گذشته، این بدافزار تمام داده‌ها را در حافظه‌ی کامپیوتر (RAM) برای جلوگیری از ایجاد پرونده‌های محلی ذخیره می‌کرد.

این موضوع وجود داشت و دارد و یک ویژگی برنامه‌ریزی شده بود بخاطر اینکه بدافزار در نظر نداشت تا داده‌های سرقت‌شده را برای مدت طولانی در کامپیوتر قربانی

نگهداری کند و از این رو نام این بدافزار Fast POS است.
نسخه‌ی جدید بدافزار از یک سازوکار در ویندوز با نام Mailslots سوءاستفاده می‌کند. Mailslots شبه پرونده‌هایی (پرونده‌های موقتی) هستند که تنها در داخل حافظه‌ی RAM قرار داشته و برای ذخیره‌ی ارتباطات بین فرآیندها استفاده می‌شوند.
بخاطر اینکه FastPOS ماژول‌های خود را بین فرآیندهایی همچون explorer.exe و services.exe تزریق می‌کند، این دسترسی را دارد تا Mailslots را ایجاد کرده و داده‌های سرقت‌شده را در آن ذخیره کند.

FastPOS کسب‌وکارهای کوچک را هدف قرار داده است!

بدافزار POS دیگری با نام LogPOS نیز از Mailslots برای ذخیره‌ی داده‌هایی به سرقت‌رفته از POS استفاده می‌کند. Mailslots ویندوز دقیقا با عملکرد حالت پیش‌فرض بدافزار FastPOS متناسب و مطابق است که داده‌ها را به محض اینکه کاربر روی کیبورد اینتر را فشار می‌دهد و یا از پایانه‌ی POS کارتی را می‌کشد، خارج می‌کند.
گروه ترندمیکرو توضیح می‌دهد: «این بدافزار FastPOS بر روی سرعت تاکید می‌کند و عمدتاً برای هدف قرار دادن کسب‌وکارهایی که دروازه‌های شبکه‌های آن‌ها باند کمتری دارد، طراحی شده است. بدیهی است که بدافزار FastPOS تمایل شدیدی به هدف قرار دادن کسب‌وکارهای کوچک تا متوسط دارد.»



Expert Bulletin News

Information Communication Technology

2th year 2016 | Weekly bulletin

اخبار فناوری اطلاعات و ارتباطات

هفته نامه | شماره هشتاد و دوم | سال دوم | ۱۰۴ صفحه

خبرنامه هفتگی کارشناسی

مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج