سراج

۳ مهر ۱۳۹۵

شماره ۷۹

خبرنامه کارشناسی

اخبار فناوری اطلاعات و ارتباطات

مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج

هفته نامه | شماره هفتاد و نهم | سال دوم | ۶۵ صفحه

Expert Bulletin News

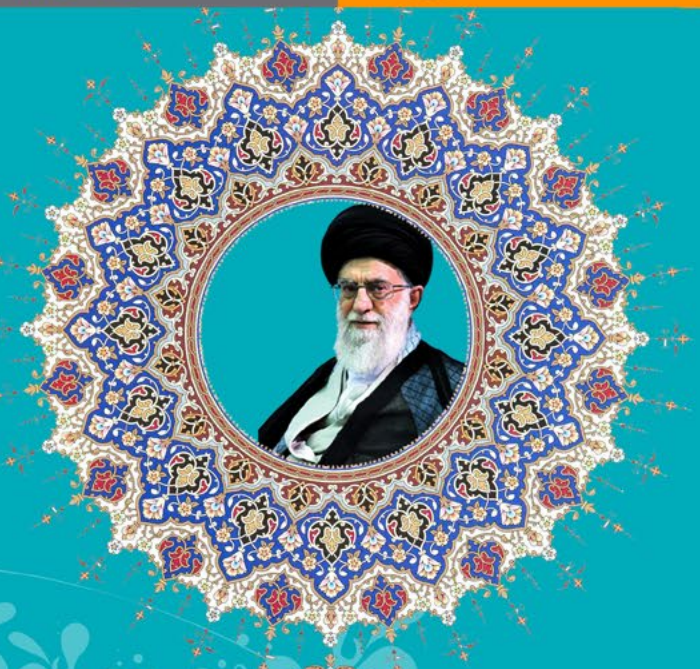
Information Communication Technology

2th year 2016 | Weekly bulletin

در این شماره می‌خوانید:

بسم الله الرحمن الرحیم

آگاهی و بصیرت



چرا نمی بینیم شعف عظیمی که دشمن پیدا می کند از آن چه که این جا از اختلاف ما، از حوادث گوناگون، از بلوای بعد از انتخابات به وجود می آید؟ اینها را باید دید. اینها را باید متوجه شد و نبایستی از دشمنی دشمن، غفلت کرد.

مقام معظم رهبری (مد ظله العالی)

فهرست مطالب

فصل اول: اخبار عمومی

فصل دوم: مدیریت امنیت

فصل سوم: سیاست سایبری

فصل چهارم: اخبار فنی

فهرست مطالب

فصل پنجم: اخبار تحلیلی

فصل اول

اخبار عمومی

اخبار عمومی

رفع 7 اشکال و آسیب‌پذیری با عرضه نسخه iOS 10 شرکت اپل

شرکت اپل سه‌شنبه پیش طی اطلاعیه‌ای از طراحی و عرضه نسخه‌های iOS 10، Xcode 8 و watchOS 3 خود خبر داد. طبق گزارش‌های منتشر شده، نسخه‌های جدید چندین آسیب‌پذیری را که منجر به بهره‌برداری‌های افشای اطلاعات، اجرای کد از راه دور و حملات منع سرویس می‌شدند، رفع کرده‌اند.

سامانه‌عامل iOS 10 به طور کلی 7 آسیب‌پذیری را رفع می‌کند. یکی از این آسیب‌پذیری‌ها که شناسه CVE-2016-4741 داشته و توسط رائول سایلز از شرکت DinoSec گزارش شده است، توسط نفوذگران برای اجرای حملات مرد میانی مورد استفاده قرار می‌گرفت و از دریافت پرونده‌های به‌روزرسانی برای دستگاه تلفن همراه جلوگیری می‌کرد. شرکت اپل این مشکل را با اجرای به‌روزرسانی از طریق اتصالات HTTPS رفع کرد.

محققان دانشگاه Politehnica در بخارست رومانی و همچنین دانشگاه کارولینای شمالی آمریکا و دانشگاه فنی Darmstadt در آلمان نیز در تحقیقات خود خبر از وجود دو آسیب‌پذیری در سامانه‌عامل iOS دادند. گزارش‌ها و تحقیقات این محققان نشان می‌دهند که برنامه‌های مخرب با استفاده آسیب‌پذیری دارای شناسه CVE-2016-4719 به موقعیت کاربر دسترسی پیدا می‌کنند و با استفاده از آسیب‌پذیری دارای شناسه CVE-2016-4620 می‌توانند مشخص کنند که کاربر در حال ارسال پیام به کدام‌یک از مخاطبان خود است.

نسخه iOS 10 علاوه بر این، یک آسیب‌پذیری مربوط به ویژگی‌های اصلاح خودکار صفحه‌کلید را رفع کرده است. این آسیب‌پذیری که دارای شناسه CVE-2016-4746 است، منجر به افشای اطلاعات محرمانه از طریق صفحه‌کلید می‌شود. این نسخه همچنین یک آسیب‌پذیری با شناسه CVE-2016-4747 را رفع کرده است که به نفوذگران این امکان را می‌دهد که از طریق انجام حملات مرد میانی، اطلاعات ورود به رایانامه کاربر را سرقت کنند. یکی از آسیب‌پذیری‌های دیگر که توسط این نسخه رفع شده است، یک اشکال با شناسه CVE-2016-4740 است که پیام‌های دستگاه‌هایی که به بخش Messages app وارد نشده باشند را به راحتی به نفوذگران نمایش می‌دهد.

علاوه بر محققان سه دانشگاه، یک محقق ناشناس دیگر نیز طی بررسی‌هایی نشان داد که در بخش پیش‌نمایش AirPrint اشکالی وجود دارد که دارای شناسه CVE-2016-4749 است و منجر به تبدیل اسناد و پرونده‌های رمزنگاری نشده به پرونده‌های موقت می‌شود.

پس از طراحی نسخه جدید iOS و نصب آن توسط کاربران، بسیاری از کاربران گزارش دادند که دستگاه‌های iPhone و iPad آن‌ها پس از اقدام برای به‌روزرسانی سامانه‌عامل به iOS 10، به مشکل برخورده‌اند. این مسئله شرکت اپل را بر آن داشت که با طراحی و عرضه نسخه iOS 10.0.1،

این مشکل را حل کند. شایان‌ذکر است که این شرکت با طراحی این نسخه، برای یک آسیب‌پذیری از مجموعه آسیب‌پذیری‌های Trident که توسط همین شرکت در ماه گذشته در نسخه iOS 9.3.5 رفع شده بود، وصله طراحی کرد.

نکته مهم در مورد نسخه‌ها و محصولات جدید شرکت اپل این است که ازآنجایی‌که سامانه عامل watchOS بر اساس سامانه‌عامل اصلی iOS کار می‌کند، اشکال دارای شناسه CVE-2016-4719 در هر دو این سامانه‌های‌عامل مشاهده می‌شود. نسخه جدید watchOS 3 این اشکال را رفع کرده است. این اشکال طبق گزارش‌ها منجر به افشای اطلاعات می‌شد.

همچنین نسخه جدید Xcode شرکت اپل دو آسیب‌پذیری را رفع کرده است. این آسیب‌پذیری‌ها به یک نفوذگر محلی این امکان را می‌دادند که در کار برنامه‌ها اختلال ایجاد کرده و یا حمله اجرای کد از راه دور را ترتیب دهند. این دو حفره امنیتی که شناسه‌های CVE-2016-4704 و CVE-2016-4705 را دارند، توسط محققانی از شرکت‌های چینی Qihoo و Tencent کشف شدند و سپس شرکت اپل در این خصوص آگاه شد.

شایان‌ذکر است که شرکت اپل در پی گزارش‌های محققان مبنی بر کشف 3 آسیب‌پذیری روز-صفرم، اقدام به‌روزرسانی فوری iOS، OS X و Safari نمود. طبق بررسی‌ها، این 3 آسیب‌پذیری برای جاسوسی علیه فعالان و گزارشگران حوزه حقوق بشر مورد استفاده قرار می گرفتند.

اخبار عمومی

شناسایی یک ابزار سوءاستفاده از دستگاه‌های خودپرداز در آمریکا با نام Periscope Skimming

سرویس مخفی ایالات متحده آمریکا طی یک هشدار به بانک‌ها و بخش‌های خدماتی دستگاه‌های خودپرداز اعلام کرد که یک نوع جدید از دستگاه‌های کلاه‌برداری از طریق خودپرداز با نام «periscope skimming» کشف شده است که طراحان آن با استفاده از یک ردیاب متصل به صفحه مدار داخلی دستگاه خودپرداز، اطلاعات مربوط به کارت‌های بانکی را مورد سوءاستفاده قرار می‌دهند.

برایان کربس، یکی از کارشناسان امنیتی مشهور در حوزه فضای مجازی در این خصوص عکس‌هایی را منتشر کرد. تصویر زیر سیم‌های بیرون آمده از این ابزار سوءاستفاده را نشان می‌دهد.

کربس در این خصوص عنوان کرد که اولین نمونه این ابزارها توسط دستگاه قضایی آمریکا شناسایی شده است. علاوه بر این، نیروهای پلیس نیز دو نمونه از این ابزارها را در آمریکا کشف کرده‌اند که نمونه اول در تاریخ ۱۹ آگوست در شهر کانکتیکات گرینویچ انگلستان و نمونه دوم نیز در ۳ سپتامبر در پنسیلوانیا آمریکا کشف شده است.

برایان کربس طی یک پست در این خصوص یادآور شد: «بر اساس یک اعلامیه هشداری که توسط یک کارگروه جرائم مالی در شهر کانکتیکات انگلستان تنظیم و به بخش‌های بانکی ارسال شده است، این نمونه کشف‌شده از دستگاه‌های سوءاستفاده از خودپردازها، از همان نمونه شناسایی‌شده در آمریکاست که در انگلستان مشاهده می‌شود. این ابزارها قادرند شماره مربوط به حداکثر ۳۲ هزار کارت پول را ذخیره کنند. علاوه بر این، این ابزارها پس از نصب روی دستگاه خودپرداز، قابلیت فعالیت تا ۱۴ روز را دارند. بررسی‌های دستگاه قضایی آمریکا در هر دو مورد کشف‌شده نشان می‌دهد که مجرمان فضای مجازی در این روش با استفاده از یک کلید ساده به بخش‌های داخلی دستگاه‌های خودپرداز دسترسی دارند و سپس با استفاده از سیم، دو بخش مهم این ابزارهای سوءاستفاده در داخل دستگاه‌های خودپرداز به هم متصل می‌شوند. یکی از این بخش‌ها، بخش ردیاب است که با استفاده از یک حفره موجود در چارچوب بخش کارت‌خوان نصب می‌شود. این ردیاب سطح کارت نقدی را به صفحه مدار متصل می‌کند. بخش دوم این دستگاه نیز «دستگاه کنترل» نامیده می‌شود که به صورت مستقیم به ردیاب متصل است و شامل یک باتری و واحد ذخیره اطلاعات است. شایان‌ذکر است که ردیاب در این فرآیند به صورتی طراحی شده است که صفحه مدار را به صفحه‌ای که اطلاعات موجود در بخش مغناطیسی پشت کارت‌های نقدی را ذخیره کرده است، متصل کند. این ردیاب سپس با استفاده از مواد بسیار چسبنده به چارچوب کارت‌خوان نصب می‌شود و در جای خود می‌ماند.»

کربس در ادامه یادآور شد: «بررسی‌های سرویس مخفی

آمریکا در این خصوص نشان می‌دهد که در هنگام باز کردن بخش‌های داخلی دستگاه خودپرداز، تنها بخشی که از این ابزار سوءاستفاده قابل‌مشاهده است، سیم‌های مربوط به ردیاب هستند که به بخش دوم این ابزار، یعنی دستگاه کنترل متصل می‌شوند.»

مسئولان در این خصوص معتقدند که نمونه‌های کشف‌شده از این ابزار صرفاً نمونه‌های اولیه هستند؛ به عبارت دیگر، این ردیاب‌ها از هیچ‌گونه دوربین مخفی و یا دیگر روش‌های لازم برای ذخیره رمز کارت‌های پولی مشتریان استفاده نکرده‌اند و دور از ذهن نیست که در نمونه‌های بعدی، از این روش‌ها استفاده شود.

کربس در این خصوص معتقد است که با توجه به استفاده روزافزون بانک‌ها از کارت‌های پرداخت پول تراشه‌ای، تعداد و میزان استفاده از چنین ابزارهایی کاهش نخواهد یافت. بسیاری از بانک‌ها و مؤسسات اعتباری نیز از بخش‌های مغناطیسی موجود در کارت‌های نقدی استفاده می‌کنند و دور از انتظار نیست که از این بخش‌های مغناطیسی برای بررسی نحوه درست وارد کردن کارت به دستگاه‌های خودپرداز استفاده شود.

کربس در ادامه یادآور شد: «دلیل اصلی استفاده از بخش‌های مغناطیسی در کارت‌های نقدی، اطمینان از واردکردن صحیح کارت‌ها به دستگاه خودپرداز است. باید توجه داشت که تا زمانی که اطلاعات مربوط به صاحب کارت نقدی در این بخش‌های مغناطیسی ذخیره می‌شود، مجرمان با استفاده از دستگاه‌های سوءاستفاده مشابه، سوءاستفاده‌های خود را به بهترین نحو انجام می‌دهند.»

سؤالی که در این بخش ممکن است در ذهن طرح شود، روش‌های جلوگیری از بروز چنین حملاتی است. در این خصوص کاربران لازم است که از دستگاه‌های خودپردازی که دسترسی به بخش‌های داخلی آن راحت است، استفاده نکنند. علاوه بر این، کاربران می‌توانند از دستگاه‌های خودپرداز موجود در بانک‌ها استفاده کنند و حتی‌الامکان از استفاده از دستگاه‌های موجود در مکان‌های محافظت نشده خودداری کنند.

اخبار عمومی

وجود یک درب پشتی در دستگاه‌های تلفن Xiaomi

یک دانشجوی هلندی رشته علوم کامپیوتر متوجه وجود یک درب پشتی در گوشی‌های شیائومی شده است که به نفوذگران امکان نصب هرگونه برنامه‌ای را در این گوشی می‌دهد. این دانشجو که تیجس برونینک نام دارد، با تحلیل این گوشی تلفن همراه متوجه این مسئله شد. وی قبل از کشف این درب پشتی، تصمیم به بررسی برنامه‌ها و خدمات از پیش نصب‌شده در ROM تلفن هوشمند خود شده بود و در تلاش بود هدف از نصب این برنامه‌ها را بیابد.

پیش از این نیز محققان امنیتی با بررسی این برنامه‌ها و خدمات از پیش نصب‌شده، در مورد خطراتی که امنیت و حریم خصوصی کاربران را تهدید می‌کنند هشدار داده بودند.

برای نمونه، شرکت امنیتی Bluebox در مارس ۲۰۱۵ به همین شکل با بررسی این برنامه‌ها، متوجه وجود برخی بدافزارها و مسائل امنیتی در گوشی‌های شیائومی Mi 4 شده بود. بررسی‌های محققان این شرکت در مورد این گوشی نشان داد که گروه‌های غیرمجاز اقدام به ساخت این گوشی کرده‌اند.

محققان شرکت امنیتی F-Secure نیز در آگوست ۲۰۱۴ با بررسی گوشی‌های جدید شیائومی RedMi 1S، متوجه شدند که این دستگاه‌ها اطلاعات کاربران را به یک کارگزار در کشور چین ارسال می‌کنند.

با توجه به این مسائل، می‌توان ادعا کرد که مشابه آنچه که برونینک کشف کرده است، در گذشته نیز مشاهده شده است. برونینک در بررسی‌های خود متوجه یک برنامه از پیش نصب‌شده مشکوک در تلفن خود شد که AnalyticsCore.apk نام داشته و به صورت ۲۴ ساعته در تلفن کار می‌کرد و کاربر نیز قادر به پاک کردن آن نبود. وی در ادامه تلاش‌هایی را برای پرسش در مورد این برنامه در تالار پشتیبانی شرکت سازنده این گوشی کرد، اما موفق نبود و به همین دلیل تصمیم گرفت با استفاده از روش‌های مهندسی معکوس روی کدها، در مورد این برنامه اطلاعاتی را به دست آورد. وی سپس کشف کرد که این برنامه هر ۲۴ ساعت اقدام به بررسی وجود پرونده‌های به‌روزرسانی از کارگزار شیائومی می‌نماید. این برنامه اطلاعات شناسایی تلفن مانند مدل، شاخصIMEI، نشانی MAC، نانس (مقدار تصادفی و دلخواه)، نام بسته‌ها و همچنین امضای تلفن‌همراه را به این کارگزار ارسال می‌کند.

این دانشجوی علوم کامپیوتر همچنین کشف کرد که اگر این برنامه در کارگزار، نرم‌افزارهای جدیدتری با نام Analytics.apk را بیابد، به صورت خودکار و بدون اجازه کاربر، اقدام به بارگیری و نصب آن می‌کند.

سؤالی که در این جا در ذهن پیش می‌آید، این است که این برنامه به چه صورت اصالت یک پرونده به‌روزرسانی را بررسی می‌کند. علاوه بر این، مشخص نیست که در

صورت اقدام مخرب یک نفوذگر و جابجایی این برنامه با یک نمونه تروجانی، چه اتفاقی خواهد افتاد.

این دانشجو طی یک پست در این خصوص عنوان کرد: «سؤالی که در اینجا پیش می‌آید این است که آیا این برنامه نرم‌افزاری درست و قانونی است یا خیر و آیا آن‌گونه که نام آن نشان می‌دهد، یک برنامه تحلیلی است یا خیر. اگر این مسائل بررسی نشود، این مسئله به این منزله است که شرکت شیائومی می‌تواند هرگونه برنامه دلخواه خود را صرفاً به دلیل اینکه نام آن Analytics.apk است، در تلفن همراه نصب کند.»

برونینک همچنین متوجه شد که فرآیند به‌روزرسانی که در این گوشی‌ها انجام می‌شود، فاقد اصل اعتبارسنجی است. این مسئله نشان می‌دهد که نفوذگران می‌توانند به راحتی با استفاده از این تلفن‌های همراه یک نرم‌افزار مخرب را ارسال کرده و با استفاده از آن بهره‌برداری‌های ممکن را انجام دهند. علاوه بر این، این مسئله نشان می‌دهد که خود شرکت سازنده می‌تواند به راحتی با تغییر نام برنامه‌های دلخواه خود به Analytics.apk، این برنامه‌ها را نصب کند.

برونینک در این خصوص عنوان کرد: «به نظر می‌رسد که شرکت شیائومی می‌تواند تنها در عرض ۲۴ ساعت هرگونه بسته و یا برنامه دلخواه خود را روی تلفن همراه نصب کند. مشخص نیست که آیا در این فرآیند بخش App Installer دخیل است یا خیر، اما می‌توان بررسی کرد که آیا می‌توان برنامه Analytics.apk را وارد تلفن همراه کرده و منتظر ماند که این برنامه به صورت خودکار نصب شود.»

این دانشجوی هلندی تاکنون به هدف اصلی این برنامه پی نبرده است، اما به نظر می‌رسد که این برنامه در اصل یک درب پشتی است که راه را برای انجام حملات مجازی توسط نفوذگران فراهم می‌کند. چنین فرآیندی می‌تواند به راحتی توسط سرویس‌های اطلاعاتی به منظور ارسال نرم‌افزارهای نظارتی به میلیون‌ها دستگاه شیائومی مورد استفاده قرار گیرد.

برونینک در این خصوص عنوان کرد: «هرطور که تصور کنیم، این مسئله، در حقیقت یک آسیب‌پذیری است.

دلیل این تصور این است که نفوذگران با داشتن شاخص IMEI و همچنین مدل تلفن شما، می‌توانند هرگونه برنامه دلخواه را روی تلفن شما نصب کنند و از این حیث، می‌توان این مسئله را یک آسیب‌پذیری تلقی کرد.»

همچنین با نگاهی ساده به مطالب عنوان‌شده در تالار شرکت در این خصوص، می‌توان موج نگرانی کاربران این شرکت را در مورد وجود این برنامه مرموز و مشکوک مشاهده کرد. یکی از این کاربران در این تالار نوشته است: «واقعاً نمی‌توان درک کرد که هدف از این برنامه چیست. حتی هنگامی که اقدام به پاک کردن آن می‌کنیم، بعد از مدتی دوباره در تلفن ظاهر می‌شود.»

کاربران در این خصوص می‌توانند با مسدود کردن تمامی اتصالات مربوط به دامنه‌های شیائومی با استفاده از برنامه‌های دیوار آتش، تا زمان پاسخ این شرکت در این خصوص منتظر باشند.

اخبار عمومی

شناسایی چندین آسیب‌پذیری در نسخه اندرویدی برنامه Signal

دو محقق امنیتی با نام‌های مارکو ورویر و ژان فیلیپ آوماسون به تازگی چندین آسیب‌پذیری را در نسخه اندرویدی برنامه پیام‌رسان امن Signal کشف کردند که نفوذگران از راه دور می‌توانند با بهره‌برداری از آن‌ها، پیوست‌های برنامه را تغییر داده و در کار آن اختلال ایجاد کنند.

برنامه Signal یک برنامه تماس صوتی و پیام‌رسان رمزنگاری‌شده، متن‌باز و رایگان است که در گوشی‌های همراه استفاده می‌شود. این برنامه دو نسخه iOS و اندروید دارد و با استفاده از پروتکل‌های رمزنگاری انتها به انتها، از ارتباطات محافظت می‌کند. این برنامه توسط شرکت Moxie Marlinspike توسعه داده شده است، اما پایه‌گذاری آن با همکاری این شرکت و شرکت Open Whisper Systems رقم خورده است.

گفتنی است کاربرانی که به دنبال یک برنامه پیام‌رسان امن هستند، می‌توانند از این برنامه استفاده کنند و امنیت ارتباطات متنی و تلفنی خود را افزایش دهند. استفاده از این برنامه رایگان است و اطلاعات کاربران در آن رمزنگاری می‌شود. مت گرین، متخصص رمزنگاری و استاد دانشگاه جانز هاپکینز، بروس اشنیر کارشناس معروف امنیتی و همچنین ادوارد اسنودن کارمند سابق سرویس جاسوسی آمریکا هر سه از این برنامه حمایت کرده‌اند. علاوه بر این، این برنامه در سریال تلویزیونی Mr. Robot نیز مورد استفاده قرار گرفته است.

ورویر و آوماسون در تحقیقات خود نسخه اندرویدی این برنامه را تحلیل کردند و دریافتند که این برنامه چندین مشکل امنیتی دارد. مهم‌ترین مشکل مشاهده‌شده در این برنامه، کد اعتبارسنجی پیام (MAC) مورد استفاده برای تائید پیوست‌ها بود. در فرآیند عادی این برنامه، با هر بار ارسال یک پرونده توسط کاربر در این برنامه، پیوست در ابتدا رمزنگاری می‌شود و سپس برنامه یک کد MAC را در این مرحله به پیوست الحاق می‌کند. این کد به منظور تائید هویت فرستنده توسط گیرنده و همچنین یکپارچگی پرونده ارسالی در این فرآیند قرار داده شده است.

پرونده پیوست شده به پیام سپس در کارگزارهای S3 Amazon ذخیره می‌شوند و می‌توان آن‌ها را با استفاده از HTTPS در دستگاه تلفن گیرنده بارگیری کرد.

این دو محقق امنیتی در این فرآیند دریافتند که می‌توان با اجرای یک حمله مرد میانی، به بخش ذخیره‌سازی Amazon S3 دسترسی پیدا کرد.

این دو همچنین در ادامه کشف کردند که می‌توان از طریق افزودن یک بایت داده به ۴ گیگابیت از پیوست، از تابع تائید کد MAC گذر کرد. این دو محقق در ادامه یادآور شدند که در عمل، ضروری نیست که نفوذگر ۴ گیگابیت اطلاعات را به کاربر ارسال کند، بلکه می‌توان با فشرده‌سازی جریان HTTP، حجم پرونده پیوست را به

تنها ۴.۵ مگابیت کاهش داد.

این دو محقق با انتشار گزارش تحلیلی خود در این خصوص اعلام کردند: «همان‌طور که مشخص است، remainingData از نوع متغیر عدد صحیح است که از کم‌کردن طول کد MAC از طول پرونده به دست می‌آید. از آنجایی‌که file.length() یک مقدار long را برمی‌گرداند و پرونده‌ها ممکن است از متغیر .Integer MAX_VALUE بزرگ‌تر باشند، remainingData می‌تواند مقدار اصلی باشد. جاوا برخلاف زبان C(++)، یک زبان حافظه امن است و به همین دلیل به هیچ وجه منجر به بروز شرایط خرابی حافظه نمی‌شود. در این شرایط می‌توان با استفاده از این سرریز، منطق برنامه را برعکس کرد. در این هنگام، اگر حجم پرونده از 4Gb + 1 byte + X بیشتر باشد، متغیر remainingDatawill برابر X خواهد شد.»

کارشناسان امنیتی همچنین یک اشکال مربوط به کلاس CallAudioManager را در برنامه شناسایی کردند. این کلاس مدیریت بسته‌های RTP توسط این برنامه را بر عهده دارد. نفوذگران از راه دور می‌توانستند با استفاده از این اشکال، این برنامه پیام‌رسان را با اختلال مواجه کنند. اشکالات شناسایی‌شده در برنامه Signal در روز ۱۳ سپتامبر گزارش شدند و شرکت طراح این برنامه در همان روز اقدام به انتشار وصله‌های لازم در گیت‌هاب نمود.

نکته‌ی شایان ذکر دیگر این است که با جستجوی ساده Google Play، می‌توان متوجه شد که این برنامه در این بخش در تاریخ ۱۶ سپتامبر عرضه شده است. این مسئله نشان می‌دهد که فروشگاه رسمی شرکت گوگل به مدت سه روز برنامه دارای اشکال را به مشتریان عرضه می‌کرده است.

فصل دوم

مدیریت امنیت

مدیریت امنیت

حمله‌ی سایبری به سازمان جهانی مبارزه با دوپینگ

سازمان جهانی مبارزه با دوپینگ (WADA) اعلام کرده که قربانی حمله‌ی سایبری شده است. آن‌ها این مسئله را به گروه جاسوسی سایبری روسی، (APT28 (Tsar Team نسبت می‌دهند.

طبق گفته‌های این سازمان، این گروه جاسوسی که با نام Fancy Bear هم شناخته می‌شوند، به پایگاه داده اداره‌ی مبارزه با دوپینگ و سامانه مدیریت (ADAMS) دسترسی پیداکرده‌اند. این گروه توانسته به مدارک محرمانه‌ی مربوط به چند ورزشکار، نظیر سایمون بایلز ژیمناست و خواهران تنیسور، ونوس و سرنا ویلیامز دسترسی پیدا کند.

اگرچه این مسئله به‌صورت رسمی توسط WADA تأیید نشده است، اما این سازمان پذیرفته که اطلاعات مهمی به دامنه‌های عمومی راه پیدا کرده است. این سازمان همچنین اضافه کرده است که عاملان حمله‌ی سایبری به WADA هشدار داده‌اند که هنوز در آغاز کار خود هستند و اسناد محرمانه‌ی بیشتری طبق گزارشات افشاء خواهد شد.

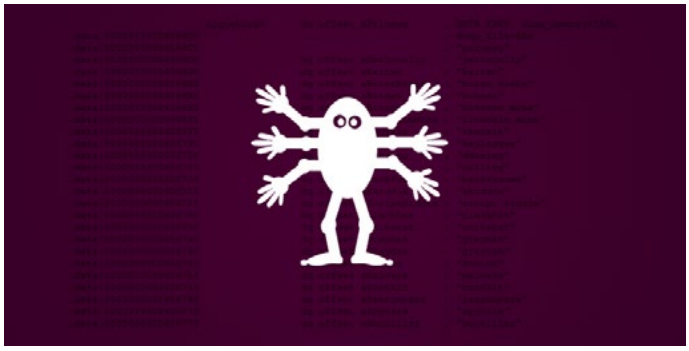
اولی ویر نیگلی، مدیر کل سازمان طی اظهاراتی بیان کرد: « WADA از این شرایط بسیار پشیمان است و از تهدیدی که مدارک محرمانه‌ی ورزشکاران را در این عمل خرابکارانه نشانه گرفته، بسیار آگاه است. WADA این‌گونه حملات سایبری را که برای تضعیف WADA و سامانه‌ی جهانی ضددوپینگ انجام می‌شود، محکوم می‌کند.»

این اخبار پیرامون صحبت‌های ماه گذشته‌ی WADA و دادگاه داوری ورزشی است. آن‌ها افشاء کرده بودند که توسط مجرمان سایبری مورد حمله قرارگرفته‌اند.

مگی دوراند، مسئول روابط عمومی WADA در گفتگو با Associated Press بیان کرد که در حال حاضر نیز نمونه‌هایی از رایانامه‌های فیشینگ به تعدادی از کاربران پایگاه‌داده مذکور ارسال شده است. مجرمان سایبری سعی داشته‌اند تا رایانامه‌ها را به‌عنوان پیامی رسمی نشان دهند و در آن‌ها درخواست به اشتراک‌گذاری جزئیات ورود کرده‌اند.

مدیریت امنیت

کشف ششمین تروجان لینوکس در طول یک ماه گذشته



کاربـران لینوکـس بایـد نگـران تروجـان دیگـری باشـند. ماننـد همیشـه، کلاه‌بـرداران از ایـن تروجـان بـرای سرقـت دسـتگاه‌هایی کـه سـامانه عامـل لینوکـس دارنـد اسـتفاده می‌کننـد. آن‌هـا از ایـن دسـتگاه‌ها بـرای راه‌انـدازی حمـلات DDoS بـر طبـق نیـاز خـود بهـره می‌جوینـد.

محققـان امنیتـی شرکـت Dr.Web کـه ایـن تهدیـد را کشـف کرده‌انـد، می‌گوینـد بـه نظـر می‌رسـد ایـن تروجـان دسـتگاه‌های لینوکـس را از طریـق آسـیب‌پذیری Shellshock کـه هنـوز در اکـثر دسـتگاه‌ها بـدون وصلـه اسـت، آلـوده می‌کنـد.

ایـن تروجـان کـه linux.DDoS.93 نـام دارد، ابتـدا پرونـده‌ی / var/run/dhcpclient-eth0.pid را به‌نوعـی تغییـر می‌دهـد تـا فرآینـد مربـوط بـه آن بـا هـر بـوت رایانـه آغـاز شـود. اگـر ایـن پرونـده وجـود نداشـت خـودش یـک نمونـه از آن را ایجـاد می‌کنـد.

هنگامی‌کـه تروجـان بـا بـوت رایانـه شروع بـه فعالیـت کنـد، از دو فرآینـد اسـتفاده خواهـد کـرد. اولیـن فرآینـد بـرای برقـراری ارتبـاط بـا کارگـزار کنـترل و فرمان‌دهـی اسـت، درحالی‌کـه دومیـن فرآینـد از فعالیـت و کارکـرد تروجـان والـد به‌صـورت دائمـی، اطمینـان پیـدا می‌کنـد.

تروجـان بـرای راه‌انـدازی حمـلات DDoS از ۲۵ فرآینـد فرزنـد اسـتفاده می‌کنـد.

مهاجمـی کـه کنـترل باتنـت تروجـان را در دسـت دارد، دسـتور حملـه را ارسـال و تروجـان ۲۵ فرآینـد فرزنـد را بـرای انجـام حملـه DDoS را راه‌انـدازی می‌کنـد.

درحال‌حـاضر، ایـن تروجـان می‌توانـد بسـته‌های UDP (بـر روی درگاه تصادفـی و یـا مشـخص)، بسـته‌های TCP (بسـته‌های سـاده یـا بـا داده‌هـای تصادفـی کـه تـا 4069 بایـت بـه هـر بسـته اضافـه می‌شـوند) و بسـته‌های HTTP (از طریـق درخواسـت‌های POST، GET، HEAD) را بـه صـورت سیل‌آسـا ارسـال کنـد.

به‌عـلاوه، ایـن تروجـان می‌توانـد خـود را به‌روزرسـانی کنـد، حـذف کنـد، فرآینـدش را پایـان دهـد، Ping ارسـال کنـد و پرونـده دریافتـی از کارگـزار کنـترل و فرمان‌دهـی را بارگیـری و اجـرا کنـد.

تروجان پس از یافتن اسم برایان کرب غیرفعال می‌شود.

تروجـان Linux.DDoS.93 همچنیـن تابعـی دارد کـه از طریق آن حافظـه‌ی رایانـه و لیسـت فرآیندهـای فعـال را پویـش می‌کنـد و اگـر بـا هرکـدام از رشـته‌های زیـر مواجـه شـود خـود را غیرفعـال می‌کنـد:

privmsg
getlocalip
kaiten
brian krebs
botnet
bitcoin mine
litecoin mine

rootkit
keylogger
ddosing
nulling
hackforums
skiddie
script kiddie
blackhat
whitehat
greyhat
grayhat
doxing
malware
bootkit
ransomware
spyware
botkiller

بیشتر این اسامی مربوط به دامنه‌ی امنیت فناوری اطلاعات هستند و احتمالا آورده شده‌اند تا مانع از انجام مهندسی معکوس توسط محققان امنیتی و یا آلوده‌شدن رایانه نویسنده این بدافزار شوند.

طی فرآیند آلوده‌سازی، تروجان دستگاه آلوده‌شده را برای پیداکردن سایر نسخه‌های خودش پویش کرده و پس از غیر فعال‌سازی آن‌ها، نسخه‌های جدیدتر را بر روی دستگاه نصب می‌کند. اهمیت این موضوع دوچندان است چرا که سامانه بروزرسانی خودکاری که آخرین نسخه تروجان را دارد شانس بیشتری برای زنده ماندن بر روی ماشین آلوده خواهد داشت.

لینوکس بستر بسیار مناسبی برای توسعه‌ی بدافزارها در طی ماه گذشته بوده است. در ۳۰ روز اخیر، محققان امنیتی ۵ تروجان دیگر لینوکس را کشف، تحلیل و آشکار کرده‌اند. این تروجان‌ها LuaBot، Mirai، PNScan، Rex و Linux.BackDoor.Irc نام دارند.

مدیریت امنیت

۶/۶ میلیون کاربر آسیب‌دیده در رخنه‌ی ClixSense

نفوذگران از طریق رخنه در سامانه‌ی شرکت ClixSense جزئیات ۶/۶ میلیون کاربر را ربوده‌اند. خدمات این شرکت شامل پرداخت پول به مشتریان برای مشاهده‌ی تبلیغات و انجام سفرهای برخط است.

تروی هانت، کارشناس امنیتی اهل استرالیا، گزارش داد که نفوذگران در ابتدای ماه به ClixSense رخنه کرده و سوابق ۶/۶ میلیون کاربر را به دست آورده‌اند و از این تعداد، ۴/۲ میلیون را در فضاهای عمومی منتشر کرده‌اند. این اطلاعات بهره‌برداری شده شامل اسامی، نام کاربری، آدرس رایانامه، کلمه‌ی عبور ذخیره‌شده در قالب متون ساده و بدون رمزنگاری، مانده‌حساب، تاریخ تولد، اطلاعات پرداخت و آدرس IP هستند.

ClixSense رخنه در سامانه‌هایش را تأیید کرده است. طبق گفته‌های این شرکت، نفوذگران پس از دسترسی به کارگزاری قدیمی که هنوز به پایگاه داده‌ای متصل بوده، توانسته‌اند به کارگزار پایگاه داده دسترسی پیدا کنند. پس از این ماجرا، کارگزار آسیب‌دیده غیرفعال شده است.

مسئولان ClixSense به کاربران اعلام کردند: «نفوذگر قادر به رونوشت‌برداری از اکثر جداول کاربران در پایگاه‌داده بوده است. او با اجرای چند کد SQL، اسامی حساب‌ها را به «حساب‌های مورد نفوذ واقع شده» تغییر داده و بسیاری از پست‌های انجمن را حذف کرده است. او همچنین مانده‌حساب کاربران را به صفر تغییر داده است.»

این شرکت اضافه کرد که: «ما قادر به بازیابی مانده‌حساب‌ها، انجمن و بسیاری از اسامی حساب‌ها بودیم. از بعضی‌ها خواسته شد تا نام خود را دوباره وارد کنند زیرا برای بازیابی اطلاعات از طریق پرونده پشتیبان، زمان زیادی برای دوباره برخط شدن صرف می‌شد.»

رمزهای عبور، بازنشانی شده و از کاربران خواسته شد تا در صورت لزوم، رمز عبور سایر حساب‌های خود را نیز تغییر بدهند. در یک پست Pastebin که پس از نفوذ حذف شد، نفوذگران ادعا کردند که پس از رخنه در یک کارگزار با امنیت بسیار کم، به ۶۶۰۶۰۰۸ سابقه‌ی کاربری و کد منبع کامل وبگاه ClixSense دسترسی پیداکرده‌اند. پس از اینکه ClixSense در ابتدا، قضیه نفوذ را انکار کرد، مهاجمان تصمیم به انتشار نمونه‌ای از داده‌ها گرفتند. مجرمان سایبری در حال فروش سایر اطلاعات به سرقت رفته از سامانه‌های شرکت هستند.

طی ماه‌های گذشته، چندین رخنه‌ی میلیونی فاش شده‌اند. فهرست سازمان‌های آسیب‌دیده شامل 33) QIP میلیون حساب آلوده‌شده)، 100) Rambler میلیون)، Mail. Ru) ۲۵ میلیون)، 100) VK میلیون)، ۴۳) Last.fm میلیون)، 2) Dota میلیون)، ۱۶۷) Linkedln میلیون)، ۳۶۰) Myspace میلیون)، ۴۵) VerticalScope میلیون)، ۶۵) Tumblr میلیون) است.

مدیریت امنیت

روش NAND Mirroring، روشی مناسب و کم‌هزینه برای رمزگشایی چند نوع از گوشی‌های اپل

یک محقق به‌تازگی با بررسی‌های خود نشان داد که فناوری NAND mirroring در گوشی آیفون متعلق به عامل تروریستی حادثه شهر سن برناردینو ایالت کالیفرنیا در آمریکا که در سال ۲۰۱۵ رخ داد، قادر بوده است از محدودیت تعداد ورود کلمه‌عبور این گوشی عبور کند.

در زمان بروز این حمله تروریستی، کشمکش و بحث میان پلیس FBI آمریکا و شرکت اپل در مورد رمزگشایی گوشی آیفون 5C مربوط به عامل تروریستی این حادثه، تبدیل به سرتیتر خبرها شد. شرکت اپل در زمان این حادثه از رمزگشایی تلفن همراه این تروریست امتناع ورزید و در طرف مقابل، پلیس FBI این شرکت را تهدید به انجام اقدامات قانونی کرد. پس از این کشمکش‌ها نیز پلیس FBI با پرداخت مبالغی، توانست گوشی تلفن همراه تروریست این حادثه را رمزشکنی کند.

کامی، رئیس پلیس FBI آمریکا در ماه آوریل طی یک نشست امنیتی در لندن اعلام کرد که برای این منظور، مبلغ ۱.۳ میلیون دلار را پرداخت کرده است. این در حالی است که پلیس FBI می‌توانست با پرداخت تنها ۱۰۰ دلار به این مهم دست پیدا کند؛ به عبارت دیگر، هر کسی می‌تواند با پرداخت این میزان، رمز گوشی آیفون خود را باز کند. سرگئی اسکوروبوگاتوف، یکی از محققان امنیتی در دانشگاه کمبریج این مسئله را اثبات کرده است.

این محقق امنیتی طی یک مقاله در این خصوص، روشی به نام NAND mirroring را معرفی کرده است که می‌توان با استفاده از آن می‌توان از محدودیت تعداد دفعات ورود رمز در گوشی‌های اپل گذر کرد. پلیس FBI در هنگام تلاش برای باز کردن قفل گوشی تروریست حادثه سن برناردینو، به این محدودیت در تعداد دفعات ورود کلمه‌عبور برخورد کرده بود.

این محقق در مقاله خود عنوان کرد: «برای این منظور، باید لحیم تراشه NAND Flash موجود در یک نمونه از این گوشی‌ها را از میان برد. به این شکل، امکان دستیابی فیزیکی به اتصالات سامانه روی تراشه فراهم می‌شود. علاوه بر این، می‌توان از این طریق به صورت جزئی مهندسی معکوس را روی پروتکل گذرگاه اختصاصی انجام داد. این فرآیند به‌هیچ‌وجه نیازمند صرف هزینه بالا و یا تجهیزات پیچیده نیست. ابزارهای لازم برای این فرآیند ارزان هستند و می‌توان آن‌ها را به راحتی فراهم کرد. با استفاده از این روش و همچنین فرآیند mirroring سخت‌افزاری می‌توان به راحتی محدودیت‌های موجود در تعداد دفعات ورود رمز را رفع کرد.»

روش NAND Mirroring یکی از روش‌هایی بود که به پلیس FBI پیشنهاد شده بود اما این سازمان از انجام آن خودداری کرد و همان‌طور که اسکوروبوگاتوف در اقدامات خود نشان داده است، چگونه این سازمان تصمیم اشتباهی گرفته است. رئیس پلیس FBI زمان پیشنهاد این روش مدعی شده بود که این روش عملی نیست.

اسکوروبوگاتوف فرآیند نفوذ به گوشی‌های آیفون 5C d دارای سامانه عامل iOS نسخه ۹.۳ را با ابزار بسیار ساده انجام داد. وی تراشه حافظه NAND را از صفحه مدار آیفون جدا کرده و داده‌ها را بر روی یک بورد آزمایشی بارها رونویسی کرد.

وی پس از این مراحل، با استفاده از جستجوی فراگیر به تحلیل تصویر داده‌های استخراج شده پرداخت. محققان دیگر در این خصوص معتقدند که اسکوروبوگاتوف کد لازم برای این کار را تنها در ۲۰ ساعت به دست آورده است. این میزان از زمان برای انجام این‌گونه حملات برای کدهای عبور ۴ رقمی لازم است و اسکوروبوگاتوف توانسته است تنها طی چند هفته، یک کد ۶ رقمی را با این روش کشف کند.

وی در مقاله خود در این خصوص خاطرنشان کرده است: «روش mirroring مطرح‌شده در این مقاله با استفاده از ابزارهای ساده که در فروشگاه‌های عادی در دسترس است، انجام شده است. بودجه لازم برای این کار تنها ۱۰۰ دلار است. شایان‌ذکر است که همین روش را می‌توان در دیگر مدل‌های آیفون پیاده کرد.»

این محقق در اقدامات خود نشان داد که روش NAND mirroring در گوشی‌های آیفون 5S و آیفون 6 که از حافظه NAND Flash استفاده می‌کنند، قابل‌اجرا است. روش NAND mirroring می‌تواند برای سایر مدل‌های آیفون که از حافظه‌های NAND Flash متفاوتی استفاده می‌کنند نیز به کار رود.

مدیریت امنیت

سوءاستفاده دوباره نفوذگران مجازی از اشکال تازه رفع شده Drupal

محققان امنیتی طی گزارش‌های خود اعلام کرده‌اند که گروهی از نفوذگران فضای مجازی به تازگی در تلاش‌اند که از یک آسیب‌پذیری بسیار خطرناک در بخش جانبی Drupal سوءاستفاده کنند. این اشکال دو ماه پیش رفع شد، اما بررسی‌ها نشان می‌دهد که بسیاری از مدیران وبگاه‌ها از وصله‌های طراحی‌شده برای این اشکال تاکنون استفاده نکرده‌اند.

این آسیب‌پذیری که ماژول سرویس‌های وب RESTful را تحت تاثیر قرار می‌دهد، طراحان را قادر می‌سازد تا موجودیت‌های Drupal را به صورت سرویس‌های وب RESTful مشاهده کنند. نسخه‌های قبل از x-2.6.7 و x-1.7.7 به نفوذگران ناشناس این امکان را می‌داد که درخواست‌های جعلی را ارسال کرده و سپس کدهای دلخواه PHP را در وبگاه‌ها اجرا کنند.

این مسئله که توسط دوین زوکزک گزارش شده است، یکی از 3 آسیب‌پذیری موجود در Drupal بوده است که در تاریخ ۱۳ جولای رفع شد. پس از این اقدام نیز یک اثبات مفهومی از بهره‌برداری و یک بخش Metasploit طراحی و منتشر شد.

مرکز Internet Storm Center موسسه SANS در این خصوص گزارش داد که تاکنون نفوذگران تلاش‌هایی را برای سوءاستفاده از این آسیب‌پذیری داشته‌اند. این موسسه در گزارش‌های خود اعلام کرد که مکانیسم‌های هانی‌پات آن اقدام به شناسایی ۴۴ تلاش برای بهره‌برداری از این آسیب‌پذیری در روز چهارشنبه کرده‌اند و بررسی نشانی‌های IP در این خصوص نشان می‌دهد که ۱۶ نشانی متفاوت این تلاش‌ها را ترتیب داده‌اند.

یوهانس بی اولریچ، عضو این مرکز در این خصوص اعلام کرد که بهره‌برداری‌های انجام‌شده به‌سادگی طراحی شده‌اند تا یک رشته را نمایش دهند. این مسئله نشان می‌دهد که نفوذگران در صدد شناسایی سامانه‌های آسیب‌پذیر هستند.

اولریچ در ادامه یادآور شد که این مرکز از جولای تلاش‌های نفوذگران در این خصوص را رصد کرده است. وی همچنین اعلام کرد که بار داده مربوط به نسخه‌های قبلی از روش‌های متفاوتی استفاده می‌کرده‌اند.

بررسی نشانی‌های IP که به این آسیب‌پذیری حمله کرده‌اند نشان می‌دهد که بیشتر این حملات علیه وبگاه‌های Drupal انجام شده است. تصور می‌شود که این وبگاه‌ها تاکنون مورد سوءاستفاده واقع شده‌اند و هم‌اکنون نیز این وبگاه‌ها به منظور شناسایی بخش‌های آسیب‌پذیر دیگر مورد پویش واقع می‌شوند.

اولریچ در این خصوص یادآور شد: «بررسی‌های ابتدایی در این خصوص نشان می‌دهد که هیچ‌گونه محتوای مخرب در این وبگاه‌ها وجود ندارد. تصور بر این بود که برخی بخش‌های تبلیغاتی و بدافزارها در این وبگاه‌ها مشاهده شوند. در عین حال، دور از انتظار نیست که نفوذگران در این سکوت، در حال ساخت شبکه‌های نفوذ خود باشند.» شایان‌ذکر است که آسیب‌پذیری‌های Drupal حتی پس از طراحی وصله‌های لازم، باز هم مورد حمله نفوذگران و مجرمان فضای مجازی بوده است. شرکت Sucuri به تازگی گزارش داده است که یک آسیب‌پذیری با نام Drupalgeddon در این خصوص رفع شده است، اما هنوز هم توسط نفوذگران به منظور نفوذ به وبگاه‌ها مورداستفاده قرار می‌گیرد.

مدیریت امنیت

سود ۱۲۱ میلیون دلار برای گروهی کلاه‌بردار که از باج‌افزار استفاده می‌کنند!

بر اساس گزارش اخیر آزمایشگاه امنیتی McAfee که هر سه ماه منتشر می‌شود، فرد یا گروه مسئول انجام عملیات توزیع یک نمونه باج‌افزار، ۱۸۹.۸۱۳ بیت‌کوین (بیش از ۱۲۱ میلیون دلار) از فعالیت‌هایش کسب درآمد داشته است.

کارشناسان بیان می‌کنند که حساب مالی حال حاضر این کلاه‌بردار حدود ۹۴ میلیون دلار است. این بدین معنا است که کلاه‌برداران حدود ۲۷ میلیون دلار را یا برای ارتقاء کارگزارهای خود و یا سایر مخارج هزینه کرده است.

حملات باج‌افزاری نسبت به سال گذشته ۱۲۸% افزایش داشته‌اند

طبق داده‌های منتشر شده از سوی McAfee، مجموع کل آلودگی‌های باج‌افزاری ۱۲۸ درصد در سال افزایش پیدا کرده است. هر سه ماه، کارشناسان امنیتی شرکت، نسخه‌های جدید باج‌افزار را می‌یابند و در هر دوره این تعداد نسبت به دوره‌ی پیش بیشتر می‌شوند. اگرچه آلودگی‌های باج‌افزاری همه خطرناک هستند اما نوع خاصی از این حملات توجه شرکت‌های امنیتی را به خود جلب کرده و آن‌هم حملات باج‌افزاری به بیمارستان‌ها است.

شرکت McAfee، از ۲۴ مورد نام برده است که در آن، باج‌افزار کنترل شبکه بیمارستان را به دست گرفته و باعث از کارافتادن آن شده است. McAfee توضیح می‌دهد که در فوریه‌ی سال گذشته نیز به افزایش آلودگی‌های باج‌افزارها در بیمارستان اشاره کرده بوده اما اوضاع اکنون بسیار بدتر شده است.

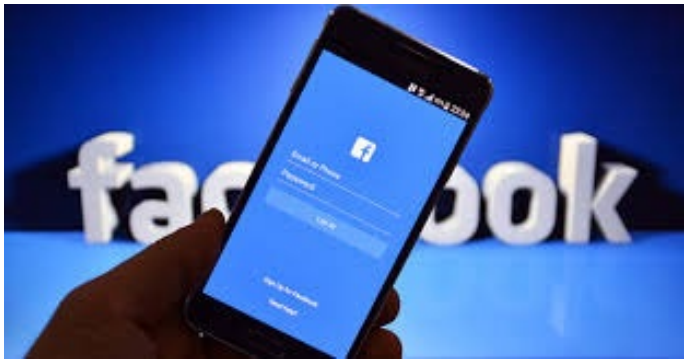
حوادثی از این قبیل نه‌تنها در ایالات‌متحده آمریکا، بلکه در بسیاری از کشورها گزارش شده‌اند. این فهرست شامل آلمان، بریتانیا، کره‌جنوبی و استرالیا نیز می‌شود. با این‌حال، ایالات‌متحده به دلیل داشتن سامانه‌ی مراقبت‌های پزشکی تجاری‌شده هدف موردعلاقه‌ی مهاجمان است. آلودگی در بیمارستان‌ها و کلینیک‌های سراسر ایالات‌متحده، از کلرادو تا کانزاس و از کالیفرنیا تا جورجیا، اتفاق افتاده است.

کلاه‌برداران باج‌افزار از بیمارستان، بیش از ۱۰۰.۰۰۰ دلار به دست آورده‌اند!

همان‌طور که باج‌افزار بر روی مصرف‌کنندگان خاصی هدف‌گذاری می‌کند، هدف قرار دادن بیمارستان‌ها نیز می‌تواند سودمند باشد. McAfee گزارش می‌کند که یک گروه باج‌افزاری که تمرکز خود را فقط بر روی بخش مراقبت‌های پزشکی گذاشته بوده است و توانسته ۱۰۰ هزار دلار از این تلاش به دست بیاورد. سایر نفوذگران در انجمن‌های جرائم سایبری و نفوذ زیرزمینی، این گروه را سرزنش کرده‌اند اما این مسئله، گروه مذکور و یا سایر نفوذگران را از ادامه‌ی حمله به بیمارستان‌ها و سایر واحدهای اورژانس بازنداشته است.

مدیریت امنیت

نفوذ به صفحات فیسبوک توسط یک محقق هندی



یک محقق هندی با نام آرون سورشکومار به تازگی یک آسیب‌پذیری خطرناک را در بخش مدیریت تجارت فیسبوک کشف کرده که می‌توان با بهره‌برداری از آن، هر صفحه‌ای را در این شبکه اجتماعی مورد نفوذ قرار داد.

مدیریت تجارت یکی از بخش‌های فیسبوک است که به تجارت‌های مختلف این امکان را می‌دهد که برخی دیگر از بخش‌های فیسبوک مانند صفحات و حساب‌های تبلیغاتی دسترسی کنترلی داشته و آن‌ها را به اشتراک بگذارند. این بخش علاوه بر این به مدیران این امکان را می‌دهد که بدون داشتن ارتباط با همکاران، دسترسی به این صفحات و حساب‌های تبلیغاتی را به اشتراک بگذارند.

با توجه به این مسائل، می‌توان درک بهتری از این بخش و همچنین تحقیقات سورشکومار داشت، اما قبل از آن ضروری است که در مورد مفهوم «ارجاع مستقیم ناامن به اشیاء» اطلاعاتی را کسب کرد.

طبق تعریف پروژه OWASP در این خصوص، این ارجاع هنگامی رخ می‌دهد که یک برنامه، دسترسی مستقیم به اشیاء را بر اساس ورودی‌های کاربران ممکن می‌سازد. نفوذگران نیز با استفاده از این آسیب‌پذیری می‌توانند از بخش احراز هویت عبور کرده و به‌صورت مستقیم به منابع در سامانه دسترسی داشته باشند.

در توضیح OWASP در این خصوص آمده است: «ارجاعات مستقیم ناامن به اشیاء به نفوذگران امکان گذر از احراز هویت را می‌دهند. این نفوذگران می‌توانند با تغییر مقدار پارامتر مورد استفاده برای اشاره به یک شیء، به‌صورت مستقیم به منابع دسترسی داشته باشند. نمونه‌های این منابع، موجودیت‌های پایگاه داده مربوط به دیگر کاربران، پرونده‌های موجود در سامانه هستند. به‌واسطه این امکان برای نفوذگران با توجه به این مهم فراهم می‌شود که برنامه ورودی کاربر را می‌گیرد و بدون بررسی‌های احراز هویت کافی، از این ورودی برای دسترسی به شیء استفاده می‌کند.»

سورشکومار از آسیب‌پذیری IDOR در مدیر تجارت فیسبوک استفاده کرد. آسیب‌پذیری مذکور به وی اجازه داد تا هر صفحه‌ای را در فیسبوک در کمتر از ۱۰ ثانیه به کنترل خود درآورد.

سورشکومار با استفاده از حساب تجاری خود در فیسبوک با شناسه ۹۰۷۹۷۰۵۵۵۹۸۱۵۲۴، یک شریک را به این حساب اضافه کرد. وی برای این منظور یک حساب با شناسه ۹۹۱۰۷۹۸۷۰۹۷۵۷۸۸ انتخاب کرد. وی سپس با استفاده از ابزار Burp Suite، درخواست را دریافت کرد. این ابزار به وی امکان تغییر درخواست را تغییر داد.

در زیر درخواست ایجاد شده توسط او را مشاهده می‌کنید:

```
POST /business_share/asset_to_agency/?dpr=2
HTTP/1.1

Host: business.facebook.com
```

694F7CC; act=1472469233458%2F6

parent_business_id=907970555981524&agency_id=991079870975788&asset_id=536195393199075&role=MANAGER&__user=100000771680694&__a=1&__dyn=aKU--XxaAcoaucCJDzopz8aWKFbGEW8UhrWqw-xG2G4aK2i8zFE8oqCwkoSEvmbgcFV8SmqVUzxeUW4ohAxWdwSDBzovU-eBCy8b48xicx2aGewzwEx2qEN4yECcKbBy9onwFwHCBxungXKdAw&__req=e&__be=-1&__pc=PHASED%3Abrands_pkg&fb_dtsg=AQHoLGh1HUmf%3AAQGT4fDF1-nQ&ttsta&=972851091025865817184521026870494511081rev=2530733__

او مقدار «asset id» را با مقدار صفحه هدف تغییر داد.

وی هم‌چنین مقادیر «parent_business_id» و «agency_id» را با هم عوض کرده و مقدار عبارت role را نیز به «MANAGER» تغییر داد.

parent_business_id= 991079870975788

agency_id= 907970555981524

asset_id =190313461381022

role= MANAGER

این محقق هندی در این فرآیند توانست ثابت کند که نفوذ به صفحات فیسبوک ممکن است. وی در این فرآیند اختیارات مدیریتی را در صفحه تجاری به‌دست آورد.

سورشکومار در ۲۹ آگوست ۲۰۱۶ آسیب‌پذیری مذکور را به فیسبوک اطلاع داد. فیسبوک نیز با بررسی این اشکال، متوجه وجود یک اشکال دیگر در بستر خود شد. این غول شبکه اجتماعی مبلغ ۱۶ هزار دلار را به عنوان بخشی از برنامه اشکال‌یابی خود به سورشکومار اهدا کرد

Connection: close

Content-Length: 436

Origin: https://business.facebook.com

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Content-Type: application/x-www-form-urlencoded

/ :Accept

Referer: https://business.facebook.com/settings/pages/536195393199075?business_id=907970555981524

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.8

Cookie: rc=2; datr=AWE3V-DUGNTOAy0wTGmpAXb; locale=en_GB; sb=BWE3V1vCnlxJF87yY9a8WWjP; pl=n; lu=gh2GPBnmZY1B1j_7J0Zi3nAA; c_user=100000771680694; xs=25%3A5C6rNSCaCX92MA%3A2%3A1472402327%3A4837; fr=05UM8RW0tTkDVgbSW.AWUB4pn0DvP1fQoqywWeORlj_LE.BXN2EF.IL.FfD.0.0.BXxBSo.AWXdKm2I; csm=2; s=Aa50vjfSfyFHHmC1.BXwxOY; _ga=GA1.2.1773948073.1464668667; p=-2; presence=EDvF3EtimeF1472469215EuserFA21B00771680694A2EstateFDutF1472469215051CEchFDp_5f1B00771680

مدیریت امنیت

تأمین امنیت در مرکز داده

مراکز داده همواره بخش اصلی بسیاری از سازمان‌ها محسوب می‌شوند. این مراکز مسئولیت فراهم کردن دسترسی قابل‌اطمینان و مقیاس‌پذیر به اطلاعات و برنامه‌هایی را دارند که سازمان را تشکیل می‌دهند. از آنجایی‌که این مراکز نسبت به گذشته اهمیت و ارزش بیشتری یافته‌اند، مسئله محافظت و نظارت بر آن‌ها نیز اهمیتی دو چندان یافته است. در عین حال، مراکز داده نیازها، چالش‌ها و تهدیدهای خاص خود را دارند.

هنوز هم در بسیاری موارد، امنیت مرکز داده و مجازی شده در قالب امنیت شبکه سنتی پیاده‌سازی می‌شود. مشکل اینجاست که مرکز داده مرز جداکننده شبکه خصوصی و محیط بیرونی نیست. اگرچه تغییر عملکرد مدل‌ها در این مرز جداکننده شاید رایج و امن به نظر برسد، اما این امر می‌تواند به شکاف‌های امنیتی خطرناکی منجر شود.

عبور از بخش‌بندی به سمت امنیت

راه‌حل صنعت برای استفاده از مدل مرز شبکه به همان شکل اصلی و بدون تغییر، این بود که کنترل‌های مرزی را مجازی کرده و آن‌ها را به درون مرکز داده منتقل کند.

این روش در حقیقت بر اساس امنیت مرز یعنی دیواره آتش آغاز شد. روش مذکور در ابتدا با اجرای دیواره آتش‌های سنتی در قالب ماشین‌های مجازی آغاز شد. سپس از مدل‌های بخش‌بندی مبتنی بر عامل استفاده شد که به لحاظ ساختاری به نرم‌افزار بستر مجازی‌سازی نزدیک بودند.

در هر دو این موارد، توجه اصلی روی ایجاد سیاست‌های مناسب درون مرکز داده است.

حال آنکه، ایجاد و برقراری قوانین در شبکه‌ها، برابر با به دام انداختن یک نفوذگر نیست. در مرز شبکه، عملکرد دیواره آتش به‌خودی‌خود کامل نبوده بلکه در کنار انواع روش‌های کشف تهدید و فناوری‌های پیش‌گیری مانند راهکارهای ضد بدافزاری، IDS/IPS، فیلترینگ وب تکمیل می‌شود. شایان ذکر است بسیاری از این فناوری‌های پیش‌گیری تهدید در مرز شبکه همانند دیواره‌های آتش به محیط مجازی منتقل شده‌اند.

حملات پیشرفته و حملات کامل

مشکل اینجاست که نمی‌توان گفت مرکز داده همان نسخه ارتقاء یافته مرز شبکه است. یک مرکز داده معمولاً با حملات پیچیده‌تری نسبت به مرز شبکه مواجه بوده و بدین ترتیب انواع تهدیدها و روش‌های حمله را تجربه می‌کند.

به‌طور خاص، تمرکز اصلی فناوری‌های مقابله با تهدید در محیط مرزی بر روی آلودگی اولیه است (مثل بدافزارها). حال آنکه مهاجمان پس از بهره‌برداری موفق از مرز شبکه، به مرکز داده حمله می‌کنند.

مهاجم ممکن است به دستگاه‌های متعددی نفوذ کرده و به سرقت جزئیات کاربران و یا حتی مدیران بپردازد. در

مراکز داده به‌جای بهره‌برداری و یا استفاده از بدافزار، مهاجمان تمایل دارند از اعتمادی که جلب کرده‌اند برای دسترسی به اطلاعات حساس‌تر و یا صدمه به آن‌ها استفاده کنند. این بدان معنا است که یک مرکز داده معمولاً با حملات پیچیده‌تری روبرو می‌شود که احتمالاً همراه با نشانه‌ای آشکار از وجود بدافزار یا بهره‌برداری نیست.

استفاده از روش‌های رفتاری

اینجاست که مدل‌های شناسایی تهدید رفتاری به صحنه وارد می‌شوند. در این موارد علاوه بر جستجو ساده برای شناسایی رفتارهای غیرعادی کاربر، باید به شناسایی رفتاری ابزارها و روش‌های حمله پرداخت.

نفوذ به حساب‌های مدیریتی، پیاده‌سازی درب‌های پشتی، راه‌اندازی تونل‌های مخفی و RAT ها همگی فرآیندهای استاندارد برای یک حمله مداوم هستند. همه این روش‌ها، رفتارهایی را از خود بروز می‌دهند که آن‌ها را از ترافیک عادی شبکه مجزا می‌سازد؛ به‌عبارت‌دیگر می‌توان به این فرآیند به‌عنوان نسخه تکامل‌یافته شناسایی تهدید نگاه کرد که به‌جای اسامی مخرب، بر رفتارهای مخرب تمرکز دارد. به‌جای این‌که به دنبال پیدا کردن یک بار داده مخرب خاص باشید، می‌توانید آنچه همه بار داده‌ها انجام می‌دهند را دنبال کنید.

همواره باید توجه داشت که مهاجمان از محدودیت‌های ما پیروی نمی‌کنند. حملات آن‌ها در اکثر موارد هم خود شبکه و هم مرکز داده را هدف قرار می‌دهند. تیم‌های امنیتی همیشه باید به هر دو این محیط‌ها توجه کافی نشان دهند.

برای مثال، ترافیک دستور و کنترل مخفی، شناسایی شبکه، سرقت اطلاعات ورود کاربر یا مدیر از نمونه‌هایی هستند که می‌توانند یک نفوذ معمولی را به مرکز داده گسترش دهند. هرکدام از این مراحل فرصتی برای شناسایی یک حمله محسوب می‌شود. بنابراین تیم‌های امنیتی باید تا حد امکان چنین مراحلی را قبل از رسیدن حمله به مرکز داده کشف کنند.

به همین دلیل استفاده از رویکردی واحد در امنیت که هم محیط شبکه و هم مرکز داده را شامل می‌شود ضروری است. حملات سایبری رخدادهای به هم مرتبط و پیچیده‌ای هستند. تصور این‌که پایگاه داده به لحاظ امنیتی یک موجودیت جدا است فقط و فقط به مهاجمان کمک می‌کند.

حال اگر متخصصان امنیتی، محیط شبکه و مرکز داده را به‌عنوان منابع مرتبط با هم در نظر بگیرند، می‌توانند به‌عنوان محافظ، از پیچیدگی موجود در یک حمله به نفع خود استفاده کنند. به عبارت دیگر، هر چه مراحل موجود در یک حمله بیشتر باشد، فرصت‌های شناسایی و مقابله با آن‌ها نیز بیشتر خواهد بود.

در طرف مقابل، بروز تغییرات غیرعادی در رفتار کاربر در مرکز داده، شاخص مناسب و کافی برای شناسایی یک حمله نیست و بررسی هرگونه تغییر غیرعادی نیز روشی ناکارآمد به لحاظ زمانی برای تحلیلگران خواهد بود. از طرف دیگر رفتارهایی مانند ایجاد تونل در محیط شبکه، مشاهده آثار ارتباط با یک درب‌پشتی در کارگزار مرکز داده و ذخیره‌سازی داده‌ها همه و همه نشانه‌هایی از یک حمله را نشان می‌دهند.

تمامی این مسائل نکته‌ای را خاطرنشان می‌کند و آن اینکه ما باید منحصر به فردهای مرکز داده و تهدیدهایی که با آن‌ها روبرو هستند را بشناسیم. البته باید توجه داشت این منحصر به فرد بودن موجب نمی‌شود که مرکز داده یک موجودیت جدا تلقی شود. ما باید به روش‌های حمله‌ای که مختص مراکز داده هستند اشراف داشته باشیم؛ به‌علاوه تمامی نکات امنیتی که در بخش محیط شبکه را به کار ببندیم. این مهم نیازمند یک برنامه‌ریزی دقیق است اما واقعیت آن است که امری دست‌یافتنی است.

فصل سوم

امنیت سایبری

امنیت‌سایبری

اقدام شرکت گوگل برای برگزاری یک دوره مسابقات نفوذ به اندروید

شرکت گوگل روز سه‌شنبه اعلام کرد که دور جدید مسابقات نفوذ را به زودی برگزار خواهد کرد. این شرکت در توضیح بیشتر در این خصوص عنوان کرد که محققان در این دوره از مسابقات باید آسیب‌پذیری‌های جدی و زنجیره‌های بهره‌برداری را در سامانه‌عامل اندروید شناسایی و کشف کنند. این شرکت هزارها دلار در این دوره از مسابقات به برندگان پرداخت خواهد کرد.

این دوره از مسابقات که «The Project Zero Prize» نام دارد، از ۱۴ مارس سال ۲۰۱۷ شروع خواهد شد. شرکت‌کنندگان در این مسابقه باید یک زنجیره کامل بهره‌برداری را که برای انجام حملات اجرای کد از راه دور در دستگاه‌های Nexus 6P و Nexus 5X مورد استفاده قرار می‌گیرند و تنها ابزار لازم برای آن‌ها رایانامه کاربران و شماره تلفن آن‌هاست، کشف کنند. شرکت گوگل اعلام کرده است که تنها کمکی که شرکت‌کنندگان مجاز به استفاده از آن هستند، باز کردن یک رایانامه در Gmail و یا یک پیام کوتاه در Messenger توسط کاربر است.

نکته‌ای که در خصوص این دوره از مسابقات مهم است، این است که این دوره در ۶ ماه برگزار می‌شود و افراد شرکت‌کننده در آن نباید به هیچ وجه آسیب‌پذیری‌های کشف‌شده را ذخیره کنند. نکته دیگر که شرکت‌کنندگان باید به آن توجه داشته باشند، این است که به محض کشف هرگونه اشکال، باید به بخش «ردیابی مسائل اندروید» اطلاع داده شود تا از این طریق از گزارش و ثبت آن توسط شخص دیگر جلوگیری شود. دلیل این اقدام این است که از سوءاستفاده از این آسیب‌پذیری توسط کسی که آن را برای اولین بار کشف می‌کند، جلوگیری شود.

ناتالی سیلوانوویچ، یکی از اعضای اصلی برگزارکننده این دوره در این خصوص عنوان کرد: «انگیزه اصلی شرکت گوگل از برگزاری این دوره، افزایش اطلاعات در خصوص نحوه کار اشکال‌ها و بهره‌برداری‌ها است. همواره شایعاتی در خصوص بهره‌برداری‌های از راه دور در مورد سامانه‌عامل اندروید شنیده شده، اما چنین مسئله‌ای به ندرت در عمل مشاهده می‌شود. این دوره از مسابقات نشان می‌دهد که این‌گونه مسائل چگونه در واقعیت وجود دارند و تمهیدات امنیتی چگونه در این اتفاقات، از شناسایی عوامل خطر باز می‌مانند. علاوه بر این، این دوره اطلاعات مهمی را در مورد نحوه محافظت از سوءاستفاده‌های ناشی از این اشکالات فراهم می‌کند.»

وی در ادامه عنوان کرد که یکی دیگر از دلایل برگزاری چنین دوره‌ای، رفع آسیب‌پذیری‌های خطرناک موجود در اندروید و جلوگیری از آسیب به کاربران است. شرکت گوگل نیز در این خصوص ابراز امیدواری کرده است که با برگزاری این دوره، اطلاعات آماری مهمی در خصوص میزان بروز بهره‌برداری‌ها به دست بیاید.

شایان‌ذکر است که شرکت‌کنندگانی که نتوانند در این دوره از مسابقات برنده شوند، می‌توانند در برنامه

اشـکال‌یابی در ازای پـاداش اندرویـد کـه بـه صـورت دوره‌ای برگـزار می‌شـود، شرکـت کننـد. شرکـت گـوگل پـس از پرداخـت بیـش از نیـم میلیـون دلار در ژوئـن بـرای ایـن برنامه‌هـا، اعـلام کـرد کـه میـزان مبلـغ پرداختـی بـه عنـوان جایـزه در ایـن برنامـه را تـا حداکـثر ۵۰ هـزار دلار بـه ازای ثبـت هـر اشـکال افزایـش داده اسـت.

امنیت‌سایبری

توسعه نسخه جدیدی از GovRAT برای حمله به دولت و سایر سازمان‌ها

بدافزار GovRAT یک ابزار جاسوسی سایبری قدیمی است که از سال ۲۰۱۴ در حملات نقش داشته است و طی سال‌ها توسط تهدیدکنندگان مختلف استفاده شده است. کارشناسان امنیتی شرکت کشف تهدیدات infoArmor اولین بار در سال ۲۰۱۵ این بدافزار را کشف کردند. GovRAT یک بستر نفوذ است که امکان ایجاد بدافزار را فراهم می‌کند. این بستر همراه با مجوزهای دیجیتال برای امضای کد دسته‌بندی شده است. همین مجوزهای دیجیتال اولین بار در بازار سیاه TheRealDeal Market روی شبکه Tor به فروش گذاشته شده‌اند. در سال ۲۰۱۵، GovRAT به قیمت ۱.۲۵ بیت کوین به فروش گذاشته شد اما کارشناسان مشاهده کردند که سازنده آن، این بستر را در معرض فروش خصوصی نیز گذاشته است.

مجوزهای دیجیتال GovRAT

ابزار GovRAT کد مخرب را با ابزارهای امضای کد مثل Microsoft Sign Tool، Win Trust و فناوری Authenticode امضای دیجیتال می‌کند. کارشناسان تصور می‌کنند که مشتری نهایی GovRAT گروه‌های APT هستند که کارکنان سیاسی، دیپلماتیک و نظامی بیش از ۱۵ کشور را در جهان هدف می‌گیرند.

سازنده GovRAT که با نام bestbuy وارد اینترنت می‌شود، کد منبع و مجوز دیجیتال امضای این کد را به مبلغ تقریباً ۴.۵ بیت کوین در بازار سیاه TheRealDeal به فروش گذاشته است.

دسترس‌پذیری کد منبع به هر کسی امکان می‌دهد که آن را دست‌کاری کرده، بهبود دهد و این همان اتفاقی است که در مورد GovRAT 2.0 در حال رخ دادن است. Vxers اخیراً نسخه جدیدی از RAT موسوم به GovRAT 2.0 را منتشر کرد که توسط نفوذگران برای هدف گرفتن دولت آمریکا و دیگر سازمان‌های این کشور استفاده شده است.

Govrat 2.0

پس از اولین گزارشی که توسط InfoArmor منتشر شد، Bestbuy شروع به استفاده از نام Popopret کرد.

RAT از طریق حملات فیشینگ نیزه‌ای و Drive-by-download فعال می‌شود. سازمان‌های دولتی و نظامی ازجمله قربانیان هستند. داده‌های به سرقت رفته از سازمان‌های نظامی نیز در بازار سیاه به فروش گذاشته شده‌اند.

گونه جدید از GovRAT 2.0 شامل چند ویژگی جدید از جمله بهبود روش‌های گریز از شناسایی، اجرای فرمان از راه دور، نگاشت خودکار دیسک‌های سخت و به اشتراک‌گذاری در شبکه‌ها است.

به گفته کارشناسان شرکت InfoArmor، سازمان‌های دولتی و نظامی بیش از پیش هدف نفوذگرانی قرار گرفته‌اند که از این تهدیدها استفاده می‌کنند.

در زیر فهرست کاملی از ویژگی‌های GovRAT 2.0 که توسط شرکت InfoArmor منتشر شده آمده است:

• دسترسی به کارگزار کنترل و فرماندهی با استفاده از هر مرورگری
• کامپایل کارگزار کنترل و فرماندهی برای لینوکس و یا ویندوز
• معکوس‌ناپذیری بدون کلید خصوصی. ضد اشکال‌یابی روز-صفرم
• نگاشت خودکار تمام دیسک‌های سخت و دیسک‌های شبکه
• ایجاد نقشه‌ای از پرونده‌ها برای جستجو، حتی زمانی که هدف برخط نیست.
• اجرای پوسته/ فرمان از راه دور
• بارگذاری پرونده‌ها یا بارگذاری و اجرای پرونده‌ها در هدف
• بارگیری پرونده‌ها از نقطه هدف. برای تسریع در بارگیری پرونده‌ها و رمزنگاری، در هنگام انتقال، تمام پرونده‌ها با نرم‌افزار LZMA فشرده شده‌اند.
• رمزنگاری سفارشی برای ارتباطات. هیچ دو دستگاهی از یک کلید استفاده نمی‌کنند.
• پشتیانی از SSL برای برقراری ارتباط. (برای استفاده از این ویژگی باید مجوز معتبر SSL خود را داشته باشید).
• از کتابخانه‌های SOCKS استفاده نمی‌کند. از API های ویژه ویندوز برای برقراری ارتباط استفاده می‌کند. امکان مسدودسازی وجود ندارد.
• به منظور ارتقا امنیت، کارگزار کنترل و فرمان هر بار یک کلمه عبور یک‌بار مصرف ایجاد می‌کند و کاربر با استفاده از آن وارد می‌شود.
• همراه با کد منبع یک کی‌لاگر FUD وجود دارد که کلید را به کارگزار دیگری می‌فرستد.
• این بدافزار برای کمپین‌های بلندمدت که ارتباط پایدار مورد نیاز است مناسب است.

یکی دیگر از ویژگی‌های جالب پیاده‌سازی شده در این بدافزار این است که بدافزار مذکور توانایی پخش شدن از طریق دستگاه‌های USB و به اشتراک‌گذاری در شبکه‌ها را مثل یک کرم رایانه‌ای دارد.

قیمت این بدافزار از ۱۰۰۰ دلار برای کد باینری اصلی و کد فرمان و کنترل تا ۶۰۰۰ دلار برای یک بسته کامل متغیر است. بسته کامل شامل کد منبع برای هر جزء از زیرساخت مخرب و واحدهای اضافی آن است.

کارشناسان امنیتی چندین پیشنهاد فروش را برای بسیاری از دامنه‌های دولت امریکا ازجمله .gsa.gov، va.gov، nasa .gov، nps.gov،faa.gov و state.gov و دامنه‌های مرتبط به ارتش امریکا، مثل army.mil، mail.mil، navy.mil و af.mil کشف کرده‌اند.

در این گزارش آمده است: «در یکی از انجمن‌های زیرزمینی در شبکه TOR، همان عامل مخرب در حال فروش مجوزهای به خطر افتاده مربوط به کارگزارهای FTP مؤسسات دولتی امریکا مشاهده است. علاوه بر USPS.gov، NOAA.gov و CDG.gov، این عامل چندین مجوز دیگر را برای زیردامنه‌های JPL.NASA.gov و NAVY.mil نیز به فروش گذاشته بود.»

مجوزها برای چندین حمله GovRAT 2.0 استفاده شده‌اند. کارشناسان همچنین شاهد استفاده از ۳۳۰۰۰ مجوز دیگر به سرقت رفته از مؤسسات دولتی، تحقیقاتی و آموزشی آمریکا بوده‌اند که سازنده بدافزار مذکور از طریق نفوذگری به نام PoM (اختصار عبارت Peace-of-Mind - یا peace) ارائه کرده است.

همچنین در این گزارش آمده است: «یک عامل مخرب دیگر با عنوان PoM نیز شناسایی شده است که یکی از شرکای popopret است و ۳۳۰۰۰ اطلاعات را همراه با مجوزهای مربوط به دولت امریکا و سازمان‌های مختلف تحقیقاتی و آموزشی به فروش گذاشته است. در توضیحات اطلاعیه فروش، خود او این موضوع را مطرح می‌کند که اطلاعات درهم‌سازی شده بودند اما او توانسته آن‌ها را رمزگشایی کند و به‌طور بالقوه از آن‌ها برای دسترسی به مؤسسات دیگر و نیز برای استفاده در رقابت‌های SE (مهندسی اجتماعی) و فیشینگ نیزه‌ای استفاده کند. PoM داده‌های به سرقت رفته کارکنان دولتی و نظامی را به

عاملان دیگر داده است. پس از تحلیل جامع مشخص شد که بخش زیادی از این داده‌ها از طریق نفوذ در وبگاه موسسه ملی علوم ساختمانی آمریکا (http://www.nibs.org/) در دسترس قرارگرفته‌اند. این وبگاه شامل اعضای زیادی از جامعه تحقیقاتی، آموزشی، دولتی و نظامی آمریکا است.»

امنیت‌سایبری

بی احتیاطی فروشندگان وب تاریک و لورفتن موقعیت جغرافیایی آن‌ها

برخی مجرمان فضای مجازی که در وب تاریک اقدام به فروش محصولات غیرقانونی می‌کنند، به تازگی به طرز ناشیانه‌ای ردپایی از خود به جای گذاشته‌اند. این مجرمان با بی‌احتیاطی و خالی نکردن اطلاعات EXIF موجود در پرونده‌های تصویری شرایطی را فراهم کرده‌اند تا در مقیاس وسیع از این عکس‌ها، راه برای شناسایی موقعیت جغرافیایی آنان باز شود.

کشف و شناسایی این مسئله در حقیقت نتیجه تحقیقات و مطالعه دو تن از دانشجویان دانشگاه هاروارد با نام‌های پائول لیسکر و میشائیل رز بوده است. این دو با طراحی یک نرم‌افزار مخصوص، تصاویر ذخیره‌شده در بایگانی‌های بازار سیاه را مورد پویش قرار دادند. شایان‌ذکر است که این فهرست به منظور رونوشت‌برداری از محتوای بازارهای سیاه و غیرقانونی وب تاریک و استفاده از آن‌ها برای اهداف تاریخی مورد استفاده قرار می‌گیرد.

بایگانی بازار سیاه مورد استفاده در این فرآیند توسط این دو دانشجو اطلاعاتی را از ۸۳ درگاه مختلف و همچنین ۴۰ انجمن مرتبط با این بازارهای سیاه در سال‌های ۲۰۱۳ تا ۲۰۱۵ در اختیار آن‌ها قرار داد. به طور کلی، تعداد پرونده‌های به‌دست‌آمده از این بایگانی‌ها ۴۴ میلیون پرونده با حجم ۱.۵ ترابایت بود.

این دو دانشجوی دانشگاه هاروارد در ادامه مطالعه خود، با استفاده از اسکریپت‌های بَش و پایتون، این فهرست را مورد تحلیل قرار داده و پرونده‌های تصویری آن را جدا کردند. این دو در مرحله بعدی اقدام به پویش تعداد 7522284 پرونده تصویری (پس از حذف موارد تکراری تعداد ۲۲۳۴۷۱ پرونده) کرده و دریافتند که از این میان، ۲۲۷۶ مورد تصاویری همراه با برچسب موقعیت جغرافیایی هستند. پس از حذف موارد تکراری از نتیجه نهایی، این دو دانشجو دریافتند که در ۲۲۹ تصویر از این تعداد، مجرمان فضای مجازی به طرز ناشیانه‌ای فراموش کرده‌اند فراداده‌های موجود را حذف کنند. این فراداده‌ها نه تنها شامل شرکت سازنده و مدل دوربین عکاسی مورد استفاده برای گرفتن این عکس‌ها بوده است، بلکه مختصات مکان‌یابی دقیق نیز در آن‌ها وجود داشته است.

در مرحله بعدی، این دو دانشجو با ارجاع متقابل تصاویر به همه بازارهای سیاه، کشف کردند که بیشتر تصاویر حاوی برچسب موقعیت جغرافیایی چندین بار در بازارها و تالارهای مختلف قرار داده شده‌اند. این امر نشان‌دهنده تعداد بالای عکس‌های تکراری در این انجمن‌ها بود.

علاوه بر این، این مطالعه و تحقیق نشان می‌دهد که تعداد کمی از فروشندگان فعال در وب تاریک اطلاعات هیچ‌گونه اطلاعاتی از امنیت ندارند به طوری که تصاویر همراه با برچسب‌های موقعیت جغرافیایی را بارها و بارها در این انجمن‌ها ارسال کرده‌اند.

علاوه بر این، این دو دانشجوی دانشگاه هاروارد اطلاعات جالبی از تصاویری که در بازار وب تاریک Agora بارگذاری

شده بود به دست آوردند. این دو ۹۶۳ عدد از این تصاویر را شناسایی کردند که از تاریخ ۱ ژانویه سال ۲۰۱۴ تا ۱۸ مارس همین سال در این بازار قرار داده شده‌اند و پس از این تاریخ، هیچ عکس دارای برچسب موقعیت جغرافیایی در این بازار قرار داده نشده است. لیسکر و رز در این خصوص اعلام کردند که این قطع ناگهانی احتمالاً به دلیل اقدامات متقابل مدیران این بازار در سمت کارگزارها رخ داده است. این دو در این خصوص عنوان کردند: «در بسیاری از موارد، وبگاه‌هایی مشاهده می‌شدند که تعداد ۵ تا ۱۰ عکس دارای برچسب موقعیت جغرافیایی در آن وجود داشت و این موقعیت‌ها تنها چند متر با هم اختلاف داشتند. این مسئله نشان می‌دهد که فروشندگان بازارهای سیاه در این خصوص بسیار بی‌احتیاط بوده‌اند و نمی‌توان این امر را عمدی و یا فراموشی این افراد برای خارج کردن این اطلاعات قلمداد کرد.»

این دو دانشجو بر بروز خطا و اشتباه در دو سوی این فرآیند، یعنی فروشندگان و مدیران بازارهای سیاه تأکید کرده‌اند. خطای فروشندگان در این خصوص آن است که اطلاعات EXIF را از عکس‌ها استخراج نکرده‌اند و از طرف دیگر، خطای مدیران بازارهای سیاه این است که فرآیند لازم برای پردازش عکس‌ها و استخراج خودکار این اطلاعات را پیاده‌سازی نکرده‌اند.

برای مثال، این دو از فیسبوک نام بردند که اطلاعات EXIF عکس‌های کاربران را به هنگام نمایش برای کاربران استخراج می‌کند و به منظور تحلیل‌های بیشتر، این اطلاعات را در پایگاه داده خود نگاه می‌دارد. این دو دانشجو این روش کار فیسبوک را قابل‌تمجید دانستند.

مثال دیگری که در این خصوص می‌توان از آن یاد کرد، درگاه Playpen است. Playpen که یک درگاه مستهجن کودکان در وب تاریک است، با بی‌احتیاطی در تنظیمات کارگزار وب مبتنی بر Tor خود، باعث شد که پلیس FBI به راحتی از این طریق اقدام به دستگیری مدیران این درگاه نماید. در این مثال، تنظیمات نادرست یک کارگزار باعث افشای نشانی IP واقعی این درگاه شد و مأموران FBI نیز با استفاده از این مسئله اقدام به شناسایی میزبان وب این درگاه نموده و سپس فردی که این کارگزار را اجاره کرده بود، شناسایی کردند.

در جدول زیر، نام برخی بازارهای سیاه وب تاریک و همچنین اطلاعات مربوط به تصاویر موجود در آن‌ها را می بینید.

امنیت‌سایبری

نفوذ به چهار سازمان دولتی حوزه سلامت در ایتالیا توسط گروه‌های نفوذ Anynomous

دو گروه نفوذ فضای مجازی با نام‌های Anonymous Italia و AntiSec-Italia که از گروه‌های نفوذ Anonymous هستند، به‌تازگی طی عملیات خود ۴ سازمان سلامت عمومی را در ایتالیا مورد نفوذ قرار داده و علاوه بر این، اطلاعات مربوط به دو سازمان را افشاء کرده‌اند.

این دو گروه در روز ۲۱ آگوست اطلاعات به‌دست‌آمده را به‌عنوان بخشی از یک عملیات Anonymous با نام OpSafePharma# به‌صورت برخط منتشر کردند. این عملیات در حقیقت پویشی است که تنها در کشور ایتالیا انجام می‌شود و هدف آن اعتراض به فعالیت‌های دولت در مورد بیماریADHD است. گزارش‌ها در این خصوص نشان می‌دهد که بخش‌های دولتی حتی برای نمونه‌های ساده این بیماری و یا قبل از انجام هرگونه فرآیند درمانی دیگر، برای این بیماری نسخه‌های دارویی سنگینی را تجویز می‌کنند.

این دو گروه نفوذ طی اعتراضات خود اعلام کرده‌اند که مسئولان دولتی و بخش‌های سلامت باید قبل از تجویز دارو، روش‌های درمانی دیگر را لحاظ کنند. علاوه بر این، این دو گروه معتقدند که دولت نباید به شرکت‌های بزرگ دارویی اجازه تأثیر بر پزشکان و درنتیجه تجویز داروهای سنگین و غیرعادی را برای درمان این بیماری بدهد.

این دو گروه پویش اعتراضی خود را در تاریخ ۱۶ مارس سال ۲۰۱۶ و در قالب انجام حملات منع سرویس در وزارت سلامت، موسسه عالی سلامت و همچنین چندین بخش دولتی سلامت ایتالیا شروع کردند.

این عملیات چند روز بعد با انجام حمله و رخنه در پایگاه اطلاعاتی AIFA و همچنین شاخه صلیب سرخ در ایتالیا ادامه یافت.

بررسی‌ها در این خصوص نشان می‌دهد که یکی از اعضای Anonymous با نام عملیاتی Artek مسئول انجام این حملات بوده است. گزارش‌ها نیز در این خصوص نشان می‌دهد که Artek پس از انتشار اطلاعات دو پایگاه‌داده مربوط به بخش‌های دولتی به‌صورت برخط، در تاریخ ۳۰ مارس توسط نیروهای پلیس ایتالیا دستگیر شده است.

مرحله دوم عملیات این پویش که OpSafePharma 2.0# نام دارد، در تاریخ ۱ ژوئن و پس از آن رخ داد که برخی نفوذگران Anonymous اقدام به افشای برخط اطلاعات مربوط به موسسه ملی سلامت ایتالیا کردند. جدیدترین مرحله این عملیات نیز در اواخر ماه آگوست صورت گرفت. در این مرحله، نفوذگران حملاتی را علیه درگاه عمومی MEDUSA مربوط به موسسه ملی سلامت، درمانگاه Azienda Ospedaliera Santa Maria، درمانگاه دانشگاه Naples Federico II و درمانگاه دولتی ASL TO2 در شهر تورینو ایتالیا ترتیب دادند. نفوذگرانی که به کارگزارها رخنه کرده بوده و وبگاه‌ها را از کار انداخته بودند در نهایت پرونده‌های مربوط به درمانگاه ناپل و

تورینـو را منتـشر کردنـد.

گـروه Anonymous Italia نیـز طـی اعلامیه‌هایـی خـبر از افشـای اطلاعـات مسروقـه در فیسـبوک و توییـتر داد. شرکـت امنیـت فضـای مجـازی SenseCy نیـز پـس از اعـلام ایـن خـبر توسـط ایـن گـروه نفـوذ، توانسـت بـه ایـن اطلاعـات دسترسـی پیـدا کـرده و محتـوای آن‌هـا را تحلیـل کنـد.

شرکـت SenseCy در خصـوص ایـن حمـلات اعـلام کـرد کـه نفوذگـران طـی حمـلات خـود حـدود ۲.۵ گیگابایـت اطلاعـات را افشـاء کرده‌انـد. آخریـن بررسـی در ایـن خصـوص نشـان می‌دهـد کـه ایـن اطلاعـات بیشـتر شـامل اسـناد ارتباطـات درون‌سـازمانی، اسـناد دارایـی و اطلاعـات رزومـه کارمنـدان می‌شـود. ایـن شرکـت در ادامـه یـادآور شـد کـه برخـی رونوشـت‌ها از اسـناد مربـوط بـه بیـماران را یافتـه اسـت کـه بـرای درمـان نـزد پزشـکان درمانگاه‌هـا معرفـی شـده بودنـد.

تیـم محققـان ایـن شرکـت در ایـن خصـوص عنـوان کردنـد: «بررسـی‌های SenseCy در ایـن خصـوص نشـان می‌دهـد کـه آخریـن عملیـات پویـش OperationSafePharma# توسـط گـروه AntiSec-Italia در یـک پنجـره زمانـی انجـام شـده اسـت کـه آن‌هـا موفـق شـده‌اند وبگاه‌هـا آسـیب‌پذیر در مراکـز درمانـی و بیمارسـتان‌ها را شناسـایی کننـد؛ بنابرایـن نمی‌تـوان ایـن عملیـات را نتیجـه تـلاش همه‌جانبـه و هماهنـگ مجموعه‌هـای نفـوذ بـرای انجـام یـک حملـه نفـوذ علیـه بخش‌هـای سـلامت تلقـی کـرد.»

امنیت‌سایبری

پیکربندی اشتباه وبگاه انتخاباتی دونالد ترامپ

پیکربندی اشتباه وبگاه انتخاباتی دونالد ترامپ، اطلاعات شخصی کارآموزان و احتمالاً افراد بیشتری را در دسترس عموم قرار داده است.

طبق گفته‌های کریس ویکری، محقق امنیتی MacKeeper که موفق به کشف این نقص شده است، کارکنان غول املاک و نامزد انتخاباتی ریاست جمهوری، کارگزار S3 Amazon را ناشیانه تنظیم کرده‌اند. نتیجه‌ی عملی این اشتباه این بود که هر فردی که به‌درستی پوشه و اسامی پرونده‌ها را حدس می‌زد، بدون نیاز به کلمه‌ی‌عبور قادر به بارگیری اطلاعات حساس می‌شد. این نقص اخیراً برطرف شده است.

ویکری با تأیید این اشکال، از طریق وبگاه Databreaches.net گروه ترامپ را مطلع ساخته است. پس از آن بلافاصله تنظیمات دسترسی کارگزار اعمال شده است. ویکری می‌گوید اعلان این خبر را بر کشف همه زوایای این اشکال ترجیح داده است.

ویکری نتیجه گرفت: «نهایتاً می‌توان گفت این موضوع، اشکالی قابل‌اجتناب از طرف گروه فناوری ترامپ بوده است. ما احتمالاً هرگز نخواهیم فهمید که عمق این فاجعه چقدر بوده است یا چه پرونده‌های دیگری را می‌شد پیدا کرد.»

ترامپ در طی کارزار انتخاباتی خود، به دلیل استفاده‌ی رقیبش، هیلاری کلینتون از کارگزار رایانامه‌ی شخصی ناامن، سروصدای بسیاری به پا کرد. کلینتون در زمان حضورش بر مسند وزارت امور خارجه از کارگزارهای شخصی ناامن بهره می‌برده است. اشتباه کارگزار وب گروه ترامپ خجالت‌آور است اما برخلاف اشکال کارگزار رایانامه‌ی کلینتون از نظر سیاسی لطمه‌ای به او وارد نمی‌کند.

کارشناسان امنیتی مستقل، بیان می‌کنند که اشتباهات مرتکب شده توسط گروه ترامپ در بسیاری از صنایع عادی هستند.

رابرت پیج، تست‌کننده ارشد نفوذ در شرکت Redscan توضیح می‌دهد: « آسیب‌پذیرهایی مانند آنچه در وبگاه رسمی دونالد ترامپ رخ داد بسیار عادی هستند و نفوذگران را قادر می‌سازند بدون داشتن اختیارات لازم به پرونده‌های حساس دست یابند. درحالی که در این مورد رخنه رخ داده در ظاهر خیلی جدی به نظر نمی‌رسد، نفوذهایی این چنینی درصورتی‌که نفوذگران به دنبال اهداف گسترده‌تر و در قالب حمله جستجوی فراگیر باشند، بسیار مخرب خواهد بود.»

فصل چهارم

اخبار فنی

اخبار فنی

برنامه راهنمای بازی Pokemon GO باعث روت دستگاه می‌شود!

برنامه اندرویدی که خود را به جای راهنمای بازی Pokemon GO جا می‌زند موجب روت دستگاه‌ها و نصب مخفیانه‌ی تبلیغ‌افزارها و برنامه‌های ناخواسته بر روی گوشی‌های هوشمند کاربران می‌شود.

این برنامه که راهنمای Pokémon Go نام دارد، توانسته به فروشگاه گوگل راه پیدا کند و در آنجا ۵۰۰ هزار بار توسط کاربران بارگیری و بر روی گوشی‌های همراه نصب شده است.

کسپرسکی اعلام کرده است که از طریق اندازه‌گیری داده‌های راه دور که توسط تولیدات امنیتی خود دریافت کرده، دریافته است که حداقل ۶ هزار کاربر گوشی‌های خود را روت کرده و تحت کنترل بدافزار بوده‌اند.

این تروجان در گذشته هم به فروشگاه گوگل آسیب‌زده است.

تحقیقات بیشتر نشان دادند که نسخه‌ی دیگری از این برنامه در ماه جولای در فروشگاه گوگل بارگذاری شده بوده اما بعداً حذف شده است. تروجانی مشابه با تروجان موجود در راهنمای Pokemon GO در 9 برنامه دیگر نیز پیدا شده که چندین بار تحت نام‌های مختلف در فروشگاه گوگل بارگذاری شده است.

کلاه‌بردار ناشناس، آشکارا به دنبال موج‌های مردمی است و بدافزار خود را به‌صورت برنامه‌های جانبی در هر برنامه یا بازی که در دوره‌ی خاصی محبوبیت دارد، قرار می‌دهد.

کسپرسکی می‌گوید که 9 برنامه‌ی دیگر بیش از 10 هزار بار نصب نشده‌اند اما یکی از برنامه‌ها توانسته است 100 هزار مرتبه بارگیری شود.

این تروجان کار یک برنامه‌نویس باتجربه است.

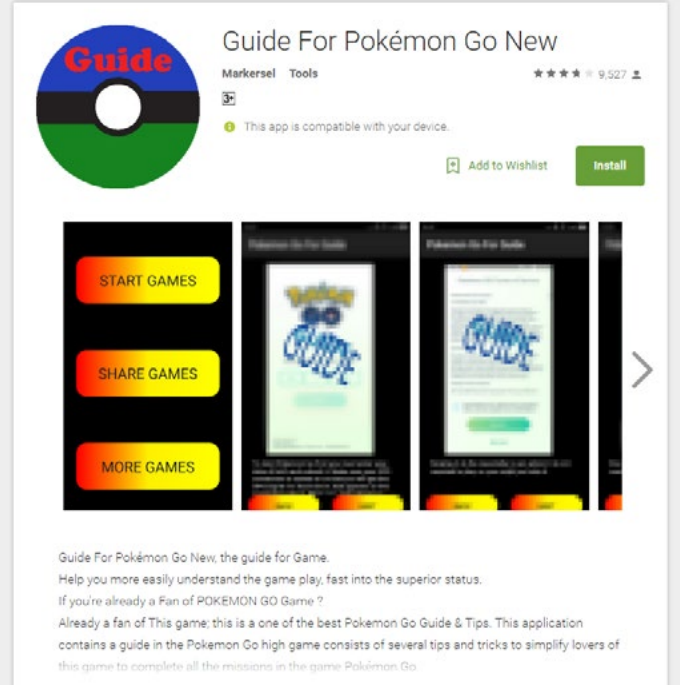
طبق تحلیل تخصصی این تروجان که کسپرسکی آن را با نام عمومی HEUR:Trojan.AndroidOS.Ztorg.ad کشف کرده است؛ بدافزار اندرویدی مذکور بسیار پیشرفته است و چندین لایه‌ی محافظتی دارد که مهندسی معکوس را بسیار سخت می‌کند. محققان بیان می‌کنند که این برنامه از بسته‌ای تجاری استفاده می‌کند. بسته‌ی تجاری برای نامنظم‌سازی و مخفی کردن کد طراحی شده تا از تحلیل محققان امنیتی جلوگیری شود. به‌علاوه، این تروجان پس از آلوده کردن یک دستگاه، بلافاصله سازندگان خود پینگ نمی‌کند. بدافزار منتظر می‌ماند تا کاربر فعالیت‌هایی نظیر نصب یا حذف نرم‌افزار دیگری را انجام دهد؛ بدین‌صورت، تروجان متوجه می‌شود که بر روی ماشین مجازی و یا شبیه‌ساز در حال اجرا نیست. این تروجان می‌تواند رفتار خرابکارانه‌ی خود را تنها درصورتی‌که مطمئن باشد دستگاه یک انسان واقعی را آلوده کرده است، نشان دهد.

یکی از حیله‌گرترین تروجان‌های تاریخ

اما حیله‌گری این تروجان تمام‌شدنی نیست. تروجان به مدت دو ساعت پس از درک واقعی بودن دستگاه، صبر

می‌کند و پس از آن با کارگزار کنترل و فرمان‌دهی ارتباط برقرار می‌کند. هنگامی‌که این اتفاق رخ داد، تروجان جزئیات دستگاه را برای ثبت قربانی جدید ارسال می‌کند و سپس منتظر فرمان می‌ماند. تروجان تا زمانی که کارگزار دو بار برای درخواست هر دستورالعمل، پاسخ ندهد عملی انجام نمی‌دهد. این مورد نیز، شیوه‌ای ضد تحلیل است تا محققان امنیتی را فریب دهد.

زمانی که کلاه‌بردار هدایت‌کننده کارگزار کنترل و فرمان تصمیم به اجرای عملیات می‌گیرد، یک پرونده‌ی JSON را با چندین پیوند ارسال می‌کند. تروجان مذکور با پیگیری این پیوندها، چندین پرونده را بر روی دستگاه آلوده بارگیری می‌کند.



تروجان بهره‌برداری‌ها را بارگیری و دستگاه را روت می‌کند

این پرونده‌ها شامل چندین بهره‌بردار اندروید هستند که قادر به روت دستگاه بوده و به مهاجم دسترسی سطح-سامانه گوشی هوشمند را می‌دهند. این بهره‌برداره‌ها از آسیب‌پذیرهای متعددی که بین سال‌های 2012 و 2015 برای روت دستگاه کشف شدند، استفاده می‌کنند. از جمله بهره‌برداری که در داده‌های انتشار یافته HackingTeam بوده است.

رومان اونوچک، تحلیلگر ارشد بدافزار و از محققان آزمایشگاه کسپرسکی، می‌گوید: «قربانیان این تروجان ممکن است حداقل در ابتدا، متوجه افزایش تبلیغ‌افزارها نشوند اما در طولانی‌مدت، پیامدهای آلودگی ممکن است بسیار بدتر باشند. اگرچه این برنامه اکنون از فروشگاه حذف شده است اما نزدیک به نیم میلیون نفر، مستعد به آلودگی هستند و امیدواریم که این اعلان، هشدار لازم را برای انجام اقدامات مورد نظر به آن‌ها بدهد.»

اخبار فنی

وصله آسیب‌پذیری مرورگر از سوی مایکروسافت

روز سه‌شنبه گذشته مایکروسافت از انتشار ۱۳ خبرنامه امنیتی خبر داد که ۵۰ آسیب‌پذیری را در ویندوز، اینترنت اکسپلورر، Edge، آفیس و Exchange وصله می‌کنند. این شرکت گفته است که یکی از آسیب‌پذیری‌های موجود در مرورگر مورد بهره‌برداری واقع شده است.

دو مورد از خبرنامه‌های حیاتی، MS16-104 و MS16-105، آسیب‌پذیری‌های ویندوز، اینترنت اکسپلورر و edge را برطرف می‌کنند. شش مورد از اشکال‌ها ازجمله CVE-2016-3351 بر هر دو مرورگر وب اینترنت اکسپلورر و Edge اثر می‌گذارند. اشکال CVE-2016-3351 یک حفره امنیتی است که به مهاجم اجازه می‌دهد اطلاعات قابل‌استفاده برای به خطر انداختن بیشتر یک سامانه هدف را به دست آورد.

اگر مهاجم بتواند قربانی را فریب بدهد تا به یک وبگاه مخرب یا در معرض خطر که میزبان یک بهره‌برداری است وارد شود می‌تواند از این اشکال افشای اطلاعات بهره‌برداری کند.

هشدار مایکروسافت نشان می‌دهد که از CVE-2016-3351 علیه کاربران اینترنت اکسپلورر استفاده شده است، اما جزئیات بیشتری را در این رابطه ارائه نکرده است. اگر مایکروسافت از طریق یک شرکت امنیتی از آسیب‌پذیری مطلع شود احتمال دارد که جزئیات حمله طی روزهای آتی به اطلاع عموم برسد.

آسیب‌پذیری‌های دیگری که توسط خبرنامه‌های MS16-104 و MS16-105 وصله شده‌اند بر اجزای مختلف اثر می‌گذارند و می‌توانند موجب افشای اطلاعات یا اجرای کد از راه دور شوند.

خبرنامه‌های حیاتی دیگر برای ویندوز عبارت‌اند از MS16-106 و MS16-116 که ۶ اشکال را برطرف می‌کنند. این اشکال‌ها می‌توانند موجب ارتقاء امتیاز، افشای اطلاعات و اجرای کد دلخواه شوند.

MS16-116 اشکال CVE-2016-3375 را برطرف می‌کند. این آسیب‌پذیری یک اشکال خرابی حافظه است که به‌واسطه شیوه دسترسی Microsoft OLE Automation و موتور برنامه‌نویسی VBScript در اینترنت اکسپلورر به اشیاء حافظه ایجاد می‌شود. اگر مهاجم بتواند قربانی را برای ورود به یک وبگاه مخرب متقاعد کند این اشکال برای اجرای کد از راه دور قابل بهره‌برداری است و با استفاده از به‌روزرسانی‌های MS16-116 و MS16-104 وصله می‌شود.

یک خبرنامه امنیتی حیاتی که برای آفیس منتشر شد (MS16-107) به آسیب‌پذیری‌های عبور ASLR، افشای اطلاعات، کلاه‌برداری در Outlook و اجرای کد از راه دور می‌پردازد.

مشکل عبور ASLR که با CVE-2016-0137 شناسایی می‌شود همان آسیب‌پذیری است که تقریباً ۹ ماه قبل توسط شرکت امنیتی enSilo به مایکروسافت اطلاع داده

شده بود. به گزارش enSilo این مشکل بر Detours اثر می‌گذارد. Detour موتوری است که بیش از ۱۰۰ شرکت از آن استفاده می‌کنند. محققان اشکال‌های مشابهی را در محصولات نرم‌افزاری چندین شرکت بزرگ شناسایی کرده‌اند.

جمعاً ۳ اشکال در Microsoft Exchange اصلاح شده‌اند که عبارت‌اند از مشکلات افشای اطلاعات، تغییر مسیر باز و ارتقای امتیاز است.

یک خبرنامه شایان‌ذکر دیگر MS16-110 است که چندین آسیب‌پذیری ویندوز را وصله می‌کند؛ ازجمله ضعفی که به مهاجم اجازه می‌دهد تا با جستجوی فراگیر درهم‌سازی کلمه عبور NTLM یک کاربر را بیابد. مایکروسافت می‌گوید جزئیات این روش حمله پیش از این برای عموم منتشر شده است.

مایکروسافت همچنین یک خبرنامه امنیتی منتشر کرد که Adobe Flash Player را در محصولات این شرکت به‌روزرسانی می‌کند. شرکت Adobe روز سه‌شنبه گفت درمجموع ۲۹ آسیب‌پذیری را در Flash Player برطرف کرده است.

اخبار فنی

اقدام شرکت موزیلا برای رفع اشکال بحرانی الصاق گواهی‌نامه در مرورگر فایرفاکس ۴۹

روز شنبه محققان خبر از وجود یک آسیب‌پذیری بحرانی در کد منبع مرورگر فایرفاکس داده بودند که به یک نفوذگر امکان می‌داد خود را به جای کارگزار موزیلا جا زده و بروزرسانی‌های جعلی را برای افزونه‌ها ارائه کند. مرورگر Tor نیز که بر مبنای یکی از نسخه‌های فایرفاکس است، روز جمعه این آسیب‌پذیری را با عرضه نسخه ۶.۰.۵ رفع کرد. مدیر ارشد بخش مهندسی امنیتی شرکت موزیلا در این خصوص اعلام کرد که تیم مهندسی امنیتی این شرکت اقدام به طراحی وصله‌های لازم برای رفع اشکال بحرانی موجود در فایرفاکس ۴۹ کرده‌اند که در روز سه‌شنبه ۲۰ سپتامبر برای کاربران عرضه خواهد شد.

مشکل اصلی در این آسیب‌پذیری، تفاوت در مکانیسم مرورگر فایرفاکس برای الصاق گواهی‌های HTTPS به‌دست‌آمده از کارگزارها با استاندارد صنعتی HPKP است.

الصاق فرآیند ارتباط یک میزبان با گواهی مورد انتظار x509 و یا کلید عمومی است. زمانی که یک کلید عمومی یا یک گواهی برای یک میزبان روشن می‌شود، این گواهی یا کلید عمومی برای میزبان مذکور الصاق می‌شود.

در این فرآیند، نفوذگری که بتواند یک گواهی جعلی ولی امضا شده برای mozila.com را در اختیار داشته باشد، می‌تواند به راحتی به‌روزرسانی‌های مخرب مربوط به افزونه‌ها را بدون بروز هیچ‌گونه هشدار و خطا مبنی بر عدم تطابق گواهی استفاده‌شده با گواهی‌های الصاق شده در مرورگر کاربر، به کاربران ارسال کند. مرورگر فایرفاکس در این شرایط تنها اقدام به بررسی دامنه گواهی‌ها کرده و کلیدهای الصاق‌شده مورد بررسی قرار نمی‌گیرند.

شرکت موزیلا طی اطلاعیه‌ای در این خصوص بیان کرد: «به دلیل بروز برخی اشکالات در این فرآیند، این شرکت با به‌روزرسانی «الصاق کلید عمومی از پیش بارگذاری شده» سعی در حل این مشکل داشته است. با توجه به این اقدام، فرآیندهای الصاق به‌روزرسانی‌های مربوط به افزونه‌ها در فایرفاکس ۴۸ که در ۱۰ سپتامبر عرضه شد، غیرفعال خواهند شد. همین شرایط برای ESR نسخه ۴۵.۳.۰ عرضه‌شده در تاریخ ۳ سپتامبر نیز برقرار خواهد بود.»

این شرکت در ادامه اذعان داشت که به منظور جلوگیری از بروز خطرات احتمالی، اقدام به تنظیم کارگزار addons.mozilla.com کرده است تا کلیدهای گواهی الصاق‌شده‌ی کاربران را هر روز به‌روزرسانی کند و از این طریق بهره‌برداری از این اشکال سخت‌تر خواهد شد.

اگرچه بسیاری از کاربران مرورگر فایرفاکس را بدون افزونه‌های موجود در آن مورداستفاده قرار می‌دهند و بدین‌ترتیب در خطر نیستند، اما مرورگر Tor با دو افزونه حیاتی توزیع شده است که حریم شخصی کاربران را

حفـظ می‌کنـد.

کاربـران ایـن مرورگـر بایـد هـر چـه سریع‌تـر مرورگـر خـود را به‌روزرسـانی کننـد. در طـرف دیگـر، کاربـران شرکـت موزیـلا بایـد افزونه‌هـا و همچنیـن بخـش به‌روزرسـانی خـودکار آن‌هـا را تـا روز سه‌شـنبه غیرفعـال کننـد.

اخبار فنی

اقدام OpenSSL مبنی بر رفع چندین آسیب‌پذیری خطرناک

پروژه‌ی penSSL روز دوشنبه اعلام کرد که به‌زودی به‌روزرسانی‌هایی را عرضه خواهد کرد که چندین آسیب‌پذیری ازجمله یک آسیب‌پذیری با خطر بالا را وصله می‌کنند.

طبق این اطلاعیه، وصله‌های لازم برای نسخه‌های 1.1.0a، 1.0.2i و 1.0.1u محصول OpenSSL در روز سه‌شنبه ۲۲ سپتامبر حدود ساعت ۸ عرضه خواهند شد. درباره این نسخه‌ها اطلاعات چندانی در دست نیست اما OpenSSL می‌گوید یکی از آسیب‌پذیری‌های کشف‌شده درجه خطر بالا را داشته است و یکی دیگر از آن‌ها درجه خطر متوسط و بقیه نیز درجه خطر کم داشته‌اند.

احتمال بهره‌برداری از اشکال‌های دارای درجه خطر بالا در مقابل آسیب‌پذیری‌های بحرانی کمتر است. توسعه‌دهندگان این شرکت به‌طورکلی پس از شناسایی اشکال‌ها، طی یک ماه اقدام به اطلاع‌رسانی درباره آن‌ها می‌کنند.

این شرکت همچنین بار دیگر به کاربران خود یادآوری کرد که پشتیبانی‌های موجود برای نسخه 1.0.1 در تاریخ ۳۱ دسامبر پایان خواهد یافت. همچنین این شرکت اعلام کرد که بخش پشتیبانی نسخه 1.1.0 از روز ۲۵ آگوست آغاز خواهد شد.

نکته‌ای که در مورد فعالیت‌های OpenSSL در خصوص آسیب‌پذیری‌ها و فرآیند رفع آن‌ها قابل‌ذکر است، این است که این شرکت سه دوره فرآیند به‌روزرسانی را طی سال جاری تا به اینجا عرضه کرده است که طی این دوره‌ها ۱۶ آسیب‌پذیری رفع شده‌اند. آخرین دوره در این خصوص در اوایل ماه می انجام شد. در این دوره، این متخصصان امنیتی شرکت یک آسیب‌پذیری با شناسه CVE-2016-2107 را که در سال ۲۰۱۳ کشف شد و مربوط به حملات Lucky 13 TLS بود، رفع کردند.

این حفره امنیتی به یک نفوذگر مرد میانی امکان می‌دهد در زمانی که اتصال موجود از رمز AES CBC استفاده کرده و کارگزار از دستورالعمل‌های AES-NI پشتیبانی می‌کند ترافیک را رمزگشایی کند. شایان‌ذکر است که تنها سه هفته پس از طراحی وصله‌های موردنیاز برای رفع این آسیب‌پذیری، محققان اعلام کردند که بسیاری از وبگاه‌های مهم در سراسر دنیا از این وصله‌ها استفاده نکرده‌اند.

نکته مهم در خصوص به‌روزرسانی‌های ماه مارس OpenSSL این است که این به‌روزرسانی‌ها به‌منظور رفع DROWN طراحی شده بودند. روش DROWN یک روش برای انجام حملات چند پروتکلی است که نفوذگران می‌توانند با استفاده از آن ارتباطات رمزنگاری‌شده را رمزگشایی کرده و اطلاعات محرمانه را به سرقت ببرند.

اخبار فنی

اقدام شرکت سیسکو مبنی بر به‌روزرسانی‌های امنیتی

شرکت سیسکو به تازگی اقدام به طراحی وصله‌هایی به منظور رفع اشکال اجرای کد از راه دور با شناسه CVE-2016-1482 کرده است. این اشکال در کارگزارهای WebEx Meetings این شرکت مشاهده می‌شود و نفوذگران ناشناس می‌توانند از راه دور فرمان‌های دلخواه را در کارگزارهای این شرکت صادر کنند.

در این خصوص، ضروری است که مدیران سامانه‌های این شرکت هر چه سریع‌تر و قبل از هرگونه اقدام نفوذگران به منظور بهره‌برداری از این آسیب‌پذیری، وصله‌های طراحی‌شده را استفاده کنند. شرکت سیسکو با بیان این مطلب خاطر نشان کرد که هیچ‌گونه راه دیگری برای کاهش و یا رفع این آسیب‌پذیری وجود ندارد. شرکت سیسکو طی یک اطلاعیه هشداری در این خصوص عنوان کرد: «به تازگی یک آسیب‌پذیری در کارگزارهای WebEx Meetings شرکت سیسکو مشاهده شده است که به نفوذگران ناشناس امکان گذر از محدودیت‌های امنیتی موجود در یک میزبان در بخش DMZ را می‌دهد. علاوه بر این، نفوذگران با استفاده از این آسیب‌پذیری می‌توانند فرمان‌های دلخواه را در یک سامانه صادر کنند.»

همان‌طور که این شرکت در این اطلاعیه اعلام کرده است، این آسیب‌پذیری نتیجه کوتاهی در فرآیند پاکسازی از اطلاعات کاربران است. نفوذگران با استفاده از این آسیب‌پذیری می‌توانند با تزریق فرمان‌های دلخواه به اسکریپت‌های یک برنامه، کارگزارهای WebEx Meetings را مورد نفوذ خود قرار دهند. شرکت سیسکو در این خصوص خاطر نشان کرد: «این آسیب‌پذیری به دلیل عدم انجام فرآیند کامل پاکسازی از اطلاعات کاربری است که توسط نرم‌افزارهای آلوده‌شده پردازش می‌شود. نفوذگران با استفاده از این آسیب‌پذیری می‌توانند با تزریق فرمان‌های دلخواه به اسکریپت برنامه‌های فعال در یک دستگاه یا سامانه و به طور اختصاصی در بخش‌های DMZ، اقدام به حمله اجرای کد دلخواه از راه دور کنند و علاوه بر این امتیازات خود را ارتقاء بخشند.» طبق اطلاعیه هشداری این شرکت، نسخه ۲.۶ این کارگزارها در معرض حملات ناشی از این آسیب‌پذیری قرار دارند.

شرکت سیسکو علاوه بر این، چندین مشکل امنیتی دیگر را در محصولات خود رفع کرده است. اشکال‌های منع سرویس که در محصولات Web Security Appliance، کارگزار WebEx Meetings، نرم‌افزار IOS XE و همچنین سامانه مسیریابی حامل مشاهده می‌شدند، از نمونه‌های این اشکالات هستند.

علاوه بر این، یکی دیگر از آسیب‌پذیری‌های خطرناکی که در کارگزار WebEx server وجود دارد، دارای شناسه CVE-2016-1483 است و ناشی از اعتبارسنجی نادرست حساب‌های کاربری در برخی بخش‌های خدماتی است. شرکت سیسکو در این خصوص عنوان کرد: «نفوذگران

ناشناس می‌توانند از راه دور و با تلاش‌های متوالی دستیابی به بخش‌های خدماتی، از این آسیب‌پذیری سوءاستفاده کنند. نتیجه این سوءاستفاده، اجرای فرآیندهای فشرده محاسباتی و رایانشی توسط سامانه است که منجر به بروز شرایط منع سرویس در آن می‌شود.»

تیم US-CERT نیز در پی رفع آسیب‌پذیری‌های یادشده توسط شرکت سیسکو، طی یک اطلاعیه با عنوان «اقدام شرکت سیسکو در به‌روزرسانی‌های امنیتی»، کاربران رایانه‌ای را از این مسئله آگاه کرده است.

اخبار فنی

شرکت SAP چندین آسیب‌پذیری را در محصول مدیریتی پایگاه داده خود وصله می‌کند!

شرکت SAP طی هفته جاری هم‌زمان با شرکت‌های Microsoft و Adobe، به‌روزرسانی‌های امنیتی ماهانه خود را به منظور رفع ۱۹ آسیب‌پذیری در محصولات خود عرضه کرد. گفتنی است که 3 مورد از این آسیب‌پذیری‌ها طی گزارش‌های این شرکت، با درجه خطر بالا قلمداد شده بودند.

رفع اشکال‌های ماه سپتامبر توسط این شرکت شامل ۱۱ یادداشت امنیتی، ۳ به‌روزرسانی برای یادداشت‌های قبلی و همچنین ۵ یادداشت بسته پشتیبانی است.

گزارش‌های این شرکت در این خصوص نشان می‌دهد که بیشتر آسیب‌پذیری‌های موجود به دلیل عدم بررسی‌های سطح اختیارات بوده است. این مشکل در بیشتر محصولات شرکت SAP مشاهده می‌شود. در عین حال، وصله‌های طراحی‌شده در این خصوص در ماه جاری آسیب‌پذیری‌هایی مانند افشای اطلاعات، منع سرویس، حملات XSS و همچنین تزریق SQL را رفع می‌کنند.

شرکت ERPScan که یک شرکت متخصص در محافظت از سامانه‌های برنامه‌ریزی منابع سازمانی شرکت‌های SAP و Oracle است، اعلام کرد که دو مورد از این سه آسیب‌پذیری جدی در کارگزار ASE شرکت SAP که یک محصول مدیریت پایگاه داده مدل رابطه‌ای است، مشاهده می‌شود. بررسی‌ها در این خصوص نشان می‌دهد که این آسیب‌پذیری‌ها مربوط به اشکال‌های تزریق SQL هستند که به نفوذگران امکان اجرای جستجوهای SQL جعلی را می‌دهند.

شرکت ERPScan طی یک پست در این خصوص یادآور شد: «کارگزار ASE اطلاعات ارزشمند و محرمانه شرکت را ذخیره می‌کند و با توجه به این مسئله، می‌توان به طور قطع ادعا کرد که پایگاه داده ASE در شرکت SAP با وجود این آسیب‌پذیری‌ها، یک گنجینه ارزشمند برای نفوذگران بوده است. در عین حال، دو آسیب‌پذیری رفع شده در این پایگاه مربوط به حملات تزریق SQL هستند. با استفاده از این آسیب‌پذیری‌ها، یک کاربر احراز هویت‌شده در کارگزار ASE می‌تواند به راحتی فرآیندهای ذخیره‌شده را با استفاده از دستورات SQL طراحی و اجرا کند.»

علاوه بر این، سومین آسیب‌پذیری خطرناکی که توسط شرکت SAP طی ماه جاری رفع شد، یک آسیب‌پذیری منع از سرویس بوده است که در محصول Business Objects BI Launchpad شناسایی شده بود.

گزارش منتشر شده از سوی ERPScan در ماه گذشته نشان می‌دهد که از ماه ژوئن سال جاری، شرکت SAP بیش از ۳۶۶۰ یادداشت امنیتی و یادداشت بسته‌های پشتیبانی را برای هزاران آسیب‌پذیری موجود عرضه کرده است.

همچنین شرکت امنیتی Onapsis نیز طی گزارشی در این خصوص بیان کرد که برخی از آسیب‌پذیری‌های موجود در محصولات SAP منجر به آلودگی بیش از ۱۰ هزار

مشتری این محصولات شده است. این شرکت در ماه می نیز هشدار داد که بیش از ۳۶ تجارت جهانی به دلیل وجود یک اشکال در یکی از محصولات SAP مورد نفوذ واقع شده‌اند. شایان‌ذکر است که این آسیب‌پذیری ۵ سال پیش وصله شده بود.

اخبار فنی

استفاده از فیلترهای DNS برای محدودسازی حملات سایبری

سیاران مارتین، رئیس مرکز اطلاعات انگلیس (GCHQ) و مرکز ملی تازه تأسیس شده‌ی امنیت سایبری (NCSC)، در برج امنیت سایبری بیلینگتون از علاقه‌ی گروه‌های جاسوسی برای استفاده از فیلترهای DNS برای ممانعت از حملات سایبری سخن گفته است. در این سخنرانی او گفت: «به دنبال انجام پروژه‌ای برای بزرگ‌تر کردن استفاده از فیلتر DNS هستیم. اگر ارائه‌کنندگان اصلی خصوصی، به‌طور مؤثر و بهتر مشتریانشان را از تماس با بدافزارهای خاص و آدرس‌های بد منع کنند، چه راهی بهتر از این به‌عنوان دفاع خودکار وجود دارد؟ بسیار مهم است که این طرح‌های اقتصادی در طرف بخش خصوصی هستند. دولت صاحب اینترنت نیست و آن را اجرا نمی‌کند. مصرف‌کنندگان حق انتخاب دارند. هرگونه فیلترینگ DNS باید به انتخاب خود فرد باشد و نگرانی‌های شخصی و انتخاب شهروندان باید در این برنامه مدنظر قرار گیرد.»

گزارش شده است که GCHQ عموماً از فیلترینگ DNS برای فیلتر کردن بخش‌هایی از اینترنت استفاده می‌کند که دولت دستور آن را می‌دهد. یکی از مورد توجه‌ترین و جدیدترین پرونده‌ها، تصمیم نخست‌وزیر سابق، دیوید کامرون برای ممنوع ساختن انواع خاصی از محتواهای هرزه‌نگاری در بریتانیا بود.

گروه‌های جاسوسی نیز اکنون در نظر دارند از روش مشابهی برای مسدود کردن آدرس‌های وب نامناسب و شناخته‌شده‌ای استفاده کنند که می‌توانند دستگاه کاربر را با بدافزار آلوده سازند. این آدرس‌ها اغلب خود را به عنوان دامنه‌های قانونی جا می‌زنند. این شیوه یکی از مرسوم‌ترین شیوه‌های انتشار جرائم سایبری است. این نوع حملات سایبری به‌طور گسترده در دولت‌های چین، ایران و روسیه برای دست‌یابی به شبکه‌های دولتی، سرقت اطلاعات یا بهره‌برداری از زیرساخت‌های ملی استفاده می‌شود. این شیوه همچنین یکی از راه‌های مرسوم برای مجرمان سایبری است که به‌طور مثال می‌توانند افراد را هدف قرار دهند و در حملات فیشینگ از آن‌ها استفاده کنند.

طبق گزارش‌ها GCHQ به دنبال همکاری با ارائه‌دهنده خدمات اینترنتی بریتانیا است تا انجام این امر را آسان سازد. اگر این اتفاق بیفتد، دیگر نیازی به مسیر طولانی و طاقت‌فرسای قانونی‌سازی این فیلترینگ نیست. شهروندان بریتانیایی به دلیل نگرانی‌های موجود پیرامون آزادی‌های شهروندی می‌توانند در این فیلترینگ شرکت نکنند.

مارتین اضافه کرد که: «این طرح آنچه را سال‌ها در امنیت سایبری به دنبالش هستیم کامل می‌کند. در بریتانیا امنیت را با طرح‌های پیش‌فرض، توسعه‌ی سخت‌افزار امن، خدمات نرم‌افزاری و دیجیتالی که شامل نقش مناسب رمزنگاری قوی است، در اختیار داریم؛ و کار خود را با شرکای بخش خصوصی برای یافتن و برطرف کردن آسیب‌پذیری

ادامه می‌دهیم. امسال تاکنون به‌صورت عمومی، اعتبار شناسایی ۲۰ آسیب‌پذیری مهم را توسط شرکت اپل و سایر ارائه‌دهندگان عمده به دست آورده‌ایم.»

فریزر کاین، رئیس SE منطقه‌ای در شرکت Bromium در گفتگو با وبگاه SCMagazineUK.com گفت: «باید از طرح‌هایی این‌چنینی حمایت کنیم چرا که گام مفیدی در جهت رسیدن به مسیر صحیح هستند؛ اما همان‌طور که تفاسیر بیان می‌کنند، این روش‌ها تنها علیه بدافزارهای ساده و شناخته‌شده به کار می‌روند. با ماهیت چندگانه‌ی بدافزارها و ازدیاد حملات هدف‌گذاری‌شده، این طرح‌ها فقط برخی از حملات کم سروصدا را فیلتر می‌کنند و کمک چندانی به حملات خطرناک حقیقی نمی‌کنند. سرمایه‌گذاری بیشتری در راه‌های عملی محافظت نیاز است که وابسته به شناسایی نیستند. امنیت مبتنی بر مجازی‌سازی در نقاط انتهایی هم بدافزارهای شناخته‌شده وهم شناخته‌نشده را جدا می‌کند. این روش باید به‌عنوان لایه‌ی بعدی دفاع در هر بخش امنیتی در نظر گرفته شود. بدون انجام این کار، امنیتی پوچ خواهیم داشت.»

این خبر زمانی اعلام شد که انجمن ارائه‌دهندگان خدمات اینترنت (ISPA، گروهی متشکل از ارائه‌دهندگان اینترنت نظیر BT، Sky و Virgin Media) اوایل این ماه نتایجی را منتشر کردند که در آن ادعا می‌شد بیشتر ارائه‌دهندگان خدمات اینترنت در بریتانیا ماهانه، هفتگی یا حتی روزانه مورد حملات سایبری قرار گرفته‌اند.

NCSC قرار است ماه آینده در لندن افتتاح شود و انتظار می‌رود تا یک همگرایی برای نیروهای امنیتی سایبری با هدف ارائه‌ی دفاع سایبری برای اقتصاد دیجیتال روزافزون بریتانیا باشد.

مت هنکاک وزیر امور خارجه در مسائل سیاست دیجیتال در بخش فرهنگ، رسانه و ورزش در ماه مارس اعلام کرده بود: «بریتانیا با تهدیدهای روبه رشد حملات سایبری از جانب دولت‌های مختلف، گروه‌های خرابکارانه مهم، گروه‌های نفوذگر و تروریست مواجه است. NCSC کمک می‌کند تا مردم، سازمان‌های بخش خصوصی و دولتی و زیرساخت‌های مهم دولتی، با امنیت بیشتری برخط شوند.

این نهاد، متخصصان سایبری را برای رفع اشکالات امنیتی سایبری گرد هم می‌آورد. این نهاد صدای قانونی امنیت اطلاعاتی در بریتانیا خواهد شد و یکی از اولین وظایفش همکاری با بانک انگلستان برای ارائه‌ی پیشنهادات به بخش مالی برای اداره‌ی مؤثرتر امنیت سایبری خواهد بود. در برپایی NCSC، از مشاوره‌های ساختاری بخش خصوصی استفاده خواهیم کرد. اهداف ما افزایش آگاهی دولت، انجام گفتگوهای حقیقی برای ارائه‌ی خدمات بهتر، تعهد جدی برای شنیدن نظرات و توسعه‌ی کانال‌های تعامل پایدار است.»

استفان گیتس، تحلیلگر اطلاعاتی تحقیقات ارشد در NSFOCUS می‌گوید: «در سراسر دنیا، مردمی که قوانین دولتشان را پیروی می‌کنند از حملات سایبری و مجرمان آن‌ها خسته شده‌اند. در بسیاری از موارد، مردم مایلند تا ارائه‌دهندگان خدمات گامی فراتر بردارند و آن‌ها را در مقابل وبگاه‌های مخرب و مشخص در اینترنت محافظت کنند. امروزه ۳۲۵ میلیون نام دامنه ثبت‌شده در تمام دامنه‌های سطح بالا و احتمالاً میلیاردها URL منحصربه‌فرد وجود دارند که از این تعداد خیلی‌ها درگیر بدافزارهای خانگی، کیت‌های بهره‌برداری، باج‌افزار، تبلیغ‌افزارهای مخرب و سایر فعالیت‌های مجرمانه هستند. هر چیزی که مردم را از رفتن ناآگاهانه به این وبگاه‌ها (که اغلب منجر به آلودگی، بهره‌برداری، کلاه‌برداری، سرقت و غیره می‌شود) محافظت کند گامی به‌سوی مسیر صحیح است. با این‌حال، انجام چنین کارهایی منجر به اشتباهاتی نظیر تهمت به دولت و ISPها برای تلاش در راستای کنترل اینترنت مردم می‌شود.»

پیرز ویلسون، رئیس مدیریت تولیدات در شرکت امنیتی Huntsman می‌گوید: «اخیراً درخواست Freedom of Information (آزادی اطلاعات) نشان داد که تعداد رخنه‌های گزارش‌شده به ICO در 12 ماه گذشته تقریباً دو برابر سال گذشته است، پس باید کاری انجام داد. برنامه‌هایی که سیاران مارتین در خصوص شبکه دفاع خودکار برای حفاظت از بریتانیا در مقابل تهدیدهای سطح پایین ارائه داده است، مطمئناً گامی در مسیر صحیح است. به علاوه این تهدیدها به‌خودی‌خود بازه‌ی وسیعی از پیچیدگی را

شامل شده و می‌توانند موجب شوند سازمان‌ها با حجم وسیعی از هشدارهای تهدیدها روبرو باشند. این امر منجر می‌شود تا تهدیدهای جدی‌تر و شرورانه‌تر بدون بررسی بمانند و کار نفوذگران حرفه‌ای‌تر هموار شود.

حل مشکل حجم تهدیدهای سطح پایین هنوز بخشی از یک جورچین است. سازمان‌ها هنوز هم درخطر حملات هدف‌گذاری‌شده و تهدیدهای داخلی قرار دارند و دیواره آتش بزرگ بریتانیا می‌تواند بخش کوچکی از مشکل را حل کند. بدین‌صورت سازمان‌ها نیاز دارند توانایی لازم را داشته باشند تا شناسایی جدی‌ترین تهدیدها امکان‌پذیر شده و بر همان اساس، تهدیدها اولویت‌بندی شوند. برای اینکه این کار بهتر انجام شود باید میزان خودکارسازی در تأیید تهدید و فرآیند کاهش آن به حداکثر برسد؛ بدین ترتیب حملات شناخته‌شده با سامانه‌های امنیتی برطرف شده و گروه‌های فناوری نیز زمان بیشتری برای تمرکز بر روی تهدیدهای جدی‌تر و ناشناخته دارند.»

فصل پنجم

اخبار تحـــلیلی

اخبار تحلیلی

تغییرات اساسی در تروجان بانکی Neverquest

تروجان بانکی Neverquest یکی از پرکارترین تروجان‌های حاضر در دنیای مجازی است که ابتدا در تابستان گذشته با استفاده از کدهای متنوع، اقدام به سوءاستفاده از رایانه کاربران می‌کرد. این تروجان اکنون با بروز تغییراتی، به روش‌های خاصی اقدام به سرقت اطلاعات کاربران از رایانه آن‌ها می‌کند. این تروجان با تزریق کد به وبگاه‌ها، اطلاعات ورود به حساب کاربران را از این وبگاه‌ها سرقت می‌کند. محققان با بررسی تغییرات و به‌روزرسانی‌های رخ‌داده در این تروجان، متوجه تغییرات بسیار زیادی در آن شده‌اند و این تغییرات زیاد، محققان را بر آن داشت که نام این تروجان را به تروجان Neverquest2 تغییر دهند. تیم واکنش و مهندسی امنیتی در شرکت Arbor Networks (ASERT) طی ماه‌های گذشته با همکاری دیگر اعضای انجمن تحقیقات امنیتی، تغییرات رخداده در تروجان Neverquest را رصد می‌کرده‌اند. بررسی‌های این محققان نشان می‌دهد که تیم طراحی کننده این تروجان با استفاده از نسخه جدید و به‌روز این تروجان با نام Neverquest2، قصد انجام حملات جدیدی را دارند.

تروجان Neverquest یکی از نسخه‌های تروجان Gozi بوده است. تروجان Gozi که چند سال پیش فعالیت خود را شروع کرد، در ابتدای فعالیت، میلیون‌ها دلار از حساب‌های بانکی کاربران را به سرقت برد. علاوه بر این، گروه بدافزاری Neverquest که با نام Vawtrak نیز شناخته می‌شوند، مدت سه سال است که در فضای مجازی فعالیت می‌کنند و در ابتدا توسط کیت بهره‌برداری Neutrino EK به سامانه‌های بانکی و رایانه‌های کاربران نفوذ می‌کردند.

محققان شرکت Arbor با بررسی نمونه‌های جدید این تروجان، اعلام کردند که به زودی یک تحلیل فنی را از این تروجان منتشر خواهند کرد. بررسی‌های این محققان تا به اکنون نشان می‌دهد که طراحان تروجان Neverquest2 تغییراتی را در این تروجان در مقایسه با نمونه‌های قبلی انجام داده‌اند. یکی از این تغییرات، افزونه‌هایی است که قادر به انتقال ۲۶۶ قاعده تزریق وب هستند که بر انواع خاصی از وبگاه‌ها اثر دارد. وبگاه‌های بانکی و مالی از نمونه وبگاه‌هایی هستند که هدف این تروجان قرار گرفته‌اند. علاوه بر این، وبگاه‌های بخش‌های دولتی، شرکت‌های خدماتی اینترنت بی‌سیم، وبگاه‌های خدمات پرداختی و وبگاه‌های جمع‌آوری اطلاعات عمومی اینترنتی نیز طبق بررسی‌ها هدف این تروجان بانکی بوده‌اند. محققان تیم ASERT علاوه بر این اعلام کرده‌اند که نکته جدید و مهمی که در این تروجان مشاهده می‌شود، وجود قوانین تزریق وب است که نفوذگران با استفاده از این ویژگی می‌توانند به وبگاه‌های تجارت بیت‌کوینی حمله کنند.

تروجان Neverquest2 همانند نمونه سابق خود قادر است به هنگام ورود کاربر به یک وبگاه مورد نفوذ این

تروجان، وارد سامانه کاربر شده و اقداماتی را در آن ترتیب دهد. این تروجان پس از این اقدامات، تزریق وب را انجام می‌دهد. در این فرآیند، این تروجان اقدام به افزودن بخش‌های اضافی به وبگاه‌ها می‌کند و از این طریق اقدام به سرقت شماره‌های شناسایی کاربران و دیگر اطلاعات محرمانه می‌نماید.

در سال ۲۰۱۴، افراد زیادی به اتهام ارتباط با این تروجان و انجام یک حمله تزریق وب دستگیر شدند. این حمله منجر به سرقت ۱.۵ میلیون دلاری در وبگاه StubHub، یکی از درگاه‌های تهیه بلیت اینترنتی شد.

تروجان Neverquest2 در تابستان سال جاری تغییراتی داشته است. شرکت امنیت فضای مجازی PhishLabs اعلام کرد که تروجان Neverquest2 از یک الگوریتم جدید تولید دامنه به منظور تولید تعداد زیادی از نام‌های دامنه استفاده می‌کند. این نام‌های دامنه توسط نفوذگران برای ایجاد ارتباط با کارگزار دستور و فرماندهی در حملات مورد استفاده قرار می‌گیرند.

یک نمونه دیگر از تغییرات مهم در این تروجان که توسط محققان تیم ASERT کشف شده است، معرفی ماژول جدید به تروجان است که قابلیت‌ها و امکانات جدیدی را به این تروجان می‌دهد. دو نمونه از این ماژول‌ها، backconnect و همچنین یک افزونه سرقت گواهی هستند که در تابستان سال جاری به این تروجان افزوده شده‌اند. ماژول backconnect (bc_32.dll) به نفوذگران امکان دستیابی از راه دور به یک سامانه آلوده را می‌دهد. این پیمانه دارای یک کارگزار VNC است که روی میزبان‌های آلوده نصب می‌شود. یکی از محققان تیم ASERT در این خصوص اعلام کرد: «نفوذگران با استفاده از رایانه‌های آلوده می‌توانند به رایانه کاربران به راحتی وارد شده و صفحه دسکتاپ کاربر را مشاهده کنند و علاوه بر این، به دوربین و همچنین سابقه مرورگرها دسترسی داشته باشند. این نفوذگران علاوه بر این، دسترسی کامل به رایانه کاربر را دارند و می‌توانند با اجرای فرمانهای CMD دلخواه و همچنین دسترسی به بخش Task Manager، اقدامات مخرب خود را انجام دهند.»

بخش دوم (dg_32.dll) که طی تابستان سال جاری به این تروجان افزوده شده است، یک بخش سرقت اطلاعات است که به جستجو و سرقت گواهی‌های ثبت‌شده در یک رایانه آلوده می‌پردازد. این افزونه طبق بررسی‌های تیم ASERT به این صورت عمل می‌کند: «این افزونه با استفاده از بخش CertOpenSystemStore() و واسطهای برنامه‌نویسی رمزنگاری‌کننده، به بخش ذخیره گواهی دسترسی پیدا می‌کنند. این بخش با کلیدهای خصوصی و مراجع صدور گواهی‌های دیجیتال در ارتباط است. این تروجان پس از این اقدام، سامانه را به منظور شناسایی حساب‌های مرورگر، کوکی‌ها و رکوردهای حافظه نهان مرورگرها مورد پویش و جستجو قرار می‌دهد.»

تیم ASERT در ادامه گزارش‌های خود عنوان کرد که نسخه جدید تروجان Neverquest2 علاوه بر این ویژگی‌ها، قادر است با دسترسی از راه دور به یک رایانه آلوده، یک تروجان دیگر با نام Pony را که به نام Fareit نیز شناخته می‌شود، در این رایانه فعال کند.

اگرچه محققان تغییرات بسیاری را در مقایسه با تروجان‌های Neverquest و Neverquest2 مشاهده می‌کنند، اما به عقیده آن‌ها، هدف اصلی این دو تروجان یکسان است. این تروجان‌ها با تغییر در صفحات وب مورد استفاده توسط کاربران، سعی در سرقت اطلاعات ورود به حساب و یا دیگر اطلاعات محرمانه کاربران دارند. محققان تیم ASERT در این خصوص معتقدند: «نمونه جدید این تروجان، یک بستر بدافزاری حرفه‌ای است که دارای بخش‌های مختلف است و نفوذگران با روش‌های خاصی اقدام به نوشتن و طراحی آن کرده‌اند. تروجان Neverquest2 در مقایسه با نمونه‌های ابتدایی تروجان Neverquest که در سال ۲۰۱۵ مشاهده شدند، توانایی‌های بسیار زیادی ندارد، اما برخی تغییرات اساسی مانند مکانیسم‌های DGA در این نمونه جدید مشاهده می‌شود. این مکانیسم که برای خصوصی‌سازی کارگزارهای دستور و کنترل این تروجان مورد استفاده قرار می‌گیرد، نشان می‌دهد که طراحان این تروجان هنوز هم در حال توسعه و گسترش این تروجان بانکی و مخرب هستند.»

اخبار تحلیلی

آلوده شدن رایانه تعدادی از کاربران به درب پشتی از طریق پرونده‌های Microsoft Publisher

محققان امنیتی شرکت Bitdefender اعلام کردند که یک زنجیره هرزنامه را کشف کرده‌اند که از طریق پرونده‌های PUB ویندوز فعال می‌شود. محققان در این خصوص اعلام کردند که این فرآیند توسط یک تروجان انجام می‌شود که یک درب پشتی را روی رایانه‌های آلوده طراحی می‌کند.

این شرکت در ادامه یادآور شد که تاکنون هزاران رایانامه را در مدت کوتاهی به این شکل شناسایی کرده است که پرونده‌های pub. به آن‌ها پیوست شده‌اند.

هرزنامه مورد استفاده در این فرآیند طبق بررسی‌ها از شرکت‌های مختلف انگلستانی و چینی به شکل سفارش و یا برگ خرید برای کاربران ارسال می‌شود.

محققان با بررسی این رایانامه‌ها دریافتند هنگامی‌که کاربر پرونده PUB را اجرا می‌کند، یک پرونده VBScript باز می‌شود و این پرونده سپس اقدام به بارگیری یک پرونده خوداستخراجی CAB در رایانه کاربر می‌کند.

این پرونده دارای یک اسکریپت AutoIt و یک پرونده رمزنگاری‌شده با الگوریتم AES-256 است. محققان شرکت Bitdefender در این خصوص اعلام کردند که زنجیره اسکریپت‌های AutoIt در این فرآیند به عنوان کلید رمزگشایی پرونده پایانی این فرآیند عمل می‌کند.

بررسی‌های بیشتر محققان در این خصوص نشان می‌دهد که پرونده رمزنگاری‌شده در حقیقت یک تروجان درب پشتی است که به طراحان خود این امکان را می‌دهد که به رایانه آلوده‌شده دسترسی پیدا کرده و به آن متصل شوند.

این تروجان قابلیت‌های مختلفی مانند کی‌لاگینگ، ثبت کلمه‌های عبور به هنگام تایپ آن‌ها توسط کاربر، رونوشت‌برداری از کلمه‌های عبور در مرورگرها و بخش‌های رایانامه‌ای، جمع‌آوری اطلاعات از رایانه آلوده‌شده و ... را دارد.

مشکلی که محققان شرکت Bitdefender به آن اذعان داشته‌اند، نام‌گذاری این تروجان است. بررسی‌های محققان تا به این لحظه نشان می‌دهد که این تروجان Generic.Malware.SFLl.545292C نام‌گذاری شده است.

پرونده‌های PUB مورد استفاده برای توزیع این تروجان نیز در اطلاعیه‌های هشداری W97M.Downloader.EGF شناسایی شده‌اند. نکته دیگری که در مورد پویش‌های توزیع این تروجان عجیب به نظر می‌رسد، استفاده از پرونده‌های PUB است. این پرونده‌ها مربوط به برنامه Microsoft Publisher که یکی از برنامه‌های موجود در محصول Office 365 suite است.

آدریان میرون، مدیر آزمایشگاه ضد هرزنامه‌ای شرکت Bitdefender در این خصوص اعلام کرد: «پرونده pub. یک پرونده عادی و رایج برای ورود بدافزارها به رایانه کاربران نیست. طراحان این حملات به دلیل اینکه کاربران کمتر به این‌گونه پرونده‌ها و میزان آلوده سازی آن‌ها شک می‌کنند، از این پرونده‌ها استفاده می‌کنند.»

اخبار تحلیلی

حمله تروجان ویندوزی Dualtoy به دستگاه‌های اندروید و iOS

محققان امنیتی به تازگی خبر از کشف یک تروجان جدید ویندوز به نام DualToy می‌دهند که از طریق اتصال USB بین یک گوشی تلفن اندروید و یک رایانه آلوده، اقدام به بارگیری جانبی برخی برنامه‌های مخرب در گوشی تلفن همراه می‌کند.

محققان شرکت Palo Alto Networks طی بررسی‌های خود اعلام کردند که این تروجان از ژانویه ۲۰۱۵ در فضای اینترنتی فعالیت داشته است و تنها به صورت نصب ناخواسته برخی برنامه‌ها و نمایش برخی تبلیغات تلفنی خود را نشان داده است. ۶ ماه بعد، این تروجان با اندکی تغییر، اقدام به حمله به دستگاه‌های اپل نمود و با هدف سرقت نام کاربری و کلمه‌های عبور بخش iTunes، اقدام به ساخت یک برنامه نامعتبر و جعلی App Store در این دستگاه‌ها کرد.

کلود خیائو، یک محقق ارشد حوزه بدافزارها با چاپ یک گزارش مبسوط و فنی در مورد این تروجان اعلام کرد: «تروجان DualToy در ابتدای ظهور خود در ژانویه ۲۰۱۵، تنها قادر به حمله به دستگاه‌های اندروید بود، اما در هفتم ژوئن سال ۲۰۱۵ اولین نمونه این تروجان که قادر به حمله به دستگاه‌های iOS است، مشاهده شد. در سال ۲۰۱۶ نیز یک نمونه دیگر از این تروجان مشاهده شد.»

محققان با بررسی روش کار این تروجان، دریافتند که این تروجان پس از آلوده کردن دستگاه ویندوز، به دنبال بخش ADB در تلفن‌های اندروید و بخش iTunes در تلفن‌های اپل می‌گردد و در مرحله بعدی، در صورت عدم وجود راه‌اندازهای مربوط به این دو بخش، اقدام به بارگیری آن‌ها می‌کند و از این طریق در هنگام برقراری اتصال، اقدام به آلوده کردن تلفن‌های همراه می‌نماید.

خیائو در این خصوص اذعان کرد: «اگرچه می‌توان با یک سری اقدامات جانبی (مانند فعال کردن بخش ADB در اندروید و جعبه شنی در اپل)، از بروز چنین حملاتی جلوگیری کرد و خطرات ناشی از این تروجان را کاهش داد، اما نحوه فعالیت این تروجان زنگ خطری برای کارشناسان و مهندسان این حوزه است. این مسئله نشان می‌دهد که نفوذگران چگونه می‌توانند با استفاده از اتصال USB، در برخی تلفن‌ها برنامه‌های جانبی مخرب را اجرا کنند. علاوه بر این، با بررسی بیشتر این تروجان می‌توان دریافت که بدافزارها چگونه می‌توانند در بسترهای مختلف پخش شوند.»

محققان همچنین طی بررسی‌های آماری خود اعلام کردند که تاکنون ۸ هزار نمونه فعال از این تروجان وجود دارد. در عین حال، آمار دقیقی از تعداد گوشی‌های آلوده به این تروجان در دست نیست.

محققان در بخش دیگری از گزارش‌های خود در این خصوص یادآور شدند که دستگاه‌های اپل در این زمینه خطر کمتری را مشاهده خواهند کرد، زیرا گواهی مربوط به بخش Apple App که تروجان برای نصب نمونه جعلی

این بخش به آن نیاز دارد، اکنون منقضی شده است.
شرکت Palo Alto نیز اذعان داشت که در طول دو سال گذشته، نمونه‌های مشابهی ثبت شده‌اند که با استفاده از ویندوز و اپل، سعی در حمله به دستگاه‌های تلفن همراه از طریق روش‌های بارگیری جانبی داشته‌اند.
خیائو در این خصوص گفت: «این نوع از حمله معروف‌ترین نوع استفاده از ابزارهای مخرب است. تروجان WireLurker که یکی از نمونه‌های مشابه این تروجان است، برنامه‌های مخرب را روی دستگاه‌های جیلبریک‌نشده‌ی آیفون اجرا می‌کرد. تروجانRCS که توسط گروه نفوذ HackingTeam طراحی شده بود نیز بدافزارهای خود را از رایانه‌ها و مک‌های آلوده به دستگاه‌های اپل جیلبریک‌شده و تلفن‌های BlackBerry ارسال می‌کرد.»
نکته مهم در خصوص تروجان DualToy این است که این تروجان تا چندی پیش تنها کاربران چینی را مورد حمله قرار می‌داد، اما تحقیقات محققان نشان می‌دهد که این تروجان به تازگی کاربرانی از کشورهای آمریکا، انگلستان، تایلند، اسپانیا و ایرلند را هدف خود قرار داده است.
خیائو در بخش دیگری از گزارش‌های خود در این خصوص اعلام کرد که برای دستگاه‌های اپل که این تروجان اقدام به آلوده‌سازی آن‌ها می‌کند، باید یک ارتباط جفتی قابل‌اعتماد میان رایانه و دستگاه تلفن همراه وجود داشته باشد. در غیر این صورت، تروجان قادر به آلوده‌سازی تلفن همراه نخواهد بود.
نکته دیگری که محققان تاکنون در کشف آن ناموفق بوده‌اند، این است که این تروجان چگونه وارد رایانه می‌شود. در عین حال، محققان مشاهده کرده‌اند که هنگامی که این تروجان وارد رایانه می‌شود، اقدام به بارگیری یک پرونده با نام adb.exe از کارگزار دستور و کنترل می‌نماید. این پرونده در حقیقت بخش اصلی ADB کاربران ویندوز است. محققان همچنین کشف کرده‌اند که نمونه‌های جدیدتر این تروجان یک پرونده محلی به همین شکل را با نام tadb.exe را در رایانه کاربر به جا می‌گذارد. این بدافزار سپس دو برنامه نصب‌کننده AppleMobileDeviceSupport64.msi و AppleApplicationSupport64.msi را که نرم‌افزارهای رسمی iTunes شرکت اپل برای نرم‌افزارهای ویندوز هستند، بارگیری می‌کند.
این تروجان در مورد دستگاه‌های اندروید، چندین برنامه نوشته‌شده به زبان چینی را در دستگاه نصب می‌کند. محققان با استفاده از این سرنخ، حدس می‌زنند که طراحان این تروجان برای این منظور، مبالغی را دریافت می‌کنند. در طرف مقابل، این تروجان در دستگاه‌های اپل با استفاده از روش‌هایی اقدام به فریب کاربران و شناسایی نام کاربری و کلمه عبور iTunes آن‌ها می‌کند.
خیائو در این خصوص اعلام کرد: « استفاده از یک برنامه جعلی App Store، کار جدیدی در این حوزه نیست. این برنامه در حال حاضر، یک برنامه جانبی مانند برنامه ZergHelper است که شرکت اپل در دستگاه‌های خود از آن استفاده می‌کند. برنامه App Store از نظر عملکرد، شبیه برنامه AceDeceiver است، زیرا هنگامی‌که برای اولین بار اجرا می‌شود، از کاربر درخواست می‌کند که شماره شناسایی و کلمه عبور خود را وارد کند.»

اخبار تحلیلی

ویژگی‌های جدید بدافزار H1N1

گزارش‌های کارشناسان امنیتی شرکت‌های سیسکو و Proofpoint و همچنین چندین محقق مستقل امنیتی نشان می‌دهد که بدافزار H1N1 در حال تغییر به یک به سارق اطلاعات است.

این بدافزار قدیمی که پیش از این به «بارگیری‌کننده بدافزار» معروف بود، نوعی از ویروس است که می‌تواند جای پای خود را در رایانه قربانی محکم کند. این ویروس توانایی گذر از نرم‌افزارهای ضدویروس را دارد و علاوه بر این، توانایی اجرا در هر بار راه‌اندازی سامانه و همچنین بارگیری و نصب بدافزارهای قوی‌تر را دارد.

گزارش شرکت سیسکو طی این هفته و همچنین گزارش شرکت Proofpoint در ماه می نشان می‌دهد که نسخه‌های جدید H1N1 ویژگی‌های بیشتری دارند و می‌توان از این حیث ادعا کرد این بدافزار در دسته بدافزارهای سارق اطلاعات جای می‌گیرد.

کارشناسان در این خصوص معتقدند که نمونه‌های جدید بدافزار H1N1 دارای توانایی جدید و قوی برای گذر از بخش کنترل دسترسی کاربر است که از طریق یک روش جدید سرقت کتابخانه لینک پویا و همچنین روش‌های مبهم‌سازی منحصر به فرد کد مهیا شده است. این روش‌ها فرآیند مهندسی معکوس را دشوارتر می‌کنند.

یکی دیگر از ویژگی‌های نسخه‌های جدید این بدافزار، ویژگی خود انتشاری آن است که توانایی ورود به دیگر رایانه‌های موجود در همان شبکه و یا درایوهای USB متصل به رایانه را به این بدافزار می‌دهد.

نکته مهم در خصوص ویژگی‌های جدید بدافزار H1N1 این است که این بدافزار قادر است اطلاعات را از سامانه‌های آلوده جمع‌آوری کرده و سپس این داده‌ها را که با استفاده از یک الگوریتم RC4 رمزنگاری شده‌اند به یک کارگزار دستور و کنترل مرکزی ارسال کند.

بدافزار H1N1 همچنین قادر است اطلاعات را از بخش‌های مختلفی در سامانه مانند اطلاعات ورود به نمایه فایرفاکس، اطلاعات Intelliform اینترنت اکسپلورر و همچنین اطلاعات ورود به رایانامه از طریق Microsoft Outlook جمع‌آوری کرده و آن‌ها را به سرقت ببرد. نکته‌ای شایان‌ذکر در این خصوص این است که اطلاعات سرقت شده توسط این بدافزار، به اندازه اطلاعات سرقت شده توسط دیگر بدافزارهای سرقت اطلاعات نیست، اما باید به یادداشت که این ویژگی به احتمال زیاد در نسخه‌های بعدی قوی‌تر خواهد شد.

محققان علاوه بر این یافته‌ها، دریافتند که این بدافزار همچنین اقدام به حذف رونوشت‌های سایه‌ای می‌کند و علاوه بر این، گزینه‌های بازیابی سامانه را نیز غیرفعال می‌کند. جاش رینالدز، از کارمندان شرکت سیسکو در این خصوص یادآور شد: «این فرمان‌ها به طور عمده توسط باج‌افزارها مورد استفاده قرار می‌گیرند، ما هنوز شواهدی را مشاهده نکرده‌ایم که H1N1 این‌گونه بدافزارها را

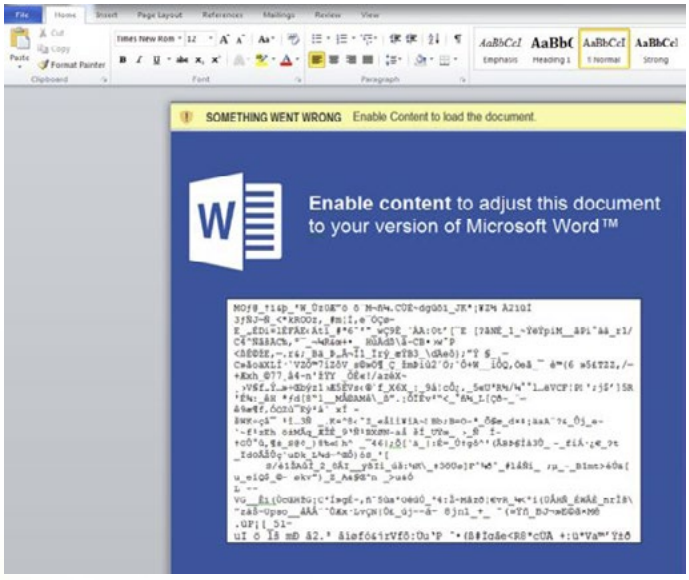
بارگیری کرده باشد.»

هرزنامه‌ای در حال توزیع سیل‌آسای H1N1

پیش از این بدافزار H1N1 در پویش‌هایی مشاهده می‌شد که تروجان بانکی Vawtrack و یا Pony را منتشر می‌کردند، اما پویش‌های جدید تنها اقدام به توزیع و پخش بدافزار H1N1 می‌کنند. شایان‌ذکر است عملکرد قرار دادن بدافزار هنوز هم در H1N1 وجود دارد و ممکن است بار دیگر توسط نفوذگران مورد استفاده قرار گیرند.

محققان شرکت سیسکو در این خصوص خبر از شناسایی یک مجموعه از هرزنامه‌ها می‌دهند که نسخه‌های جدید این بدافزار را پخش می‌کنند.

مجرمان فضای مجازی برای این منظور، پرونده‌های مخرب DOC را درون رایانامه‌ها قرار می‌دهند. پرونده مذکور از همان روش «فعال‌سازی ویرایش» استفاده می‌کند تا اسکریپت VBA موجود را اجرا کند. این اسکریپت H1N1 را بارگیری و نصب می‌کند. تصویر زیر، نمونه‌ای از پرونده‌های مخرب DOC مورد استفاده در این فرآیند را نشان می‌دهد.



پویش فعال پخش این بدافزار در حال حاضر سازمان‌های مالی، تولید انرژی، ارتباطات و بخش‌های نظامی و دولتی را هدف قرار می‌دهد. گفتنی است که این پویش برای این منظور از عناوین مختلف در رایانامه‌ها استفاده می‌کند تا کارمندان را فریب دهد.

محققان سیسکو در بخش دیگری از تحقیقات خود، با استفاده از اطلاعات موجود در بخش OpenDNS، کشف کردند که یک گروه جاسوسی پخش‌کننده این بدافزار از نشانی marekkazuewsky@gazeta.pl استفاده می‌کند، تاکنون اقدام به ثبت ۱۷۷ دامنه کرده است. این دامنه‌ها به منظور ارسال مجموعه‌های هرزنامه‌ای دارای بدافزار H1N1 مورد استفاده قرار می‌گیرد.

محققان همچنین با بررسی اطلاعات موجود در سایر پویش‌ها، توانستند این دامنه‌ها و گروه مربوط به آن را به چندین عملیات بدافزاری دیگر مرتبط کنند که به توزیع تروجان درب پشتی Bayrob، تروجان بانکی Rovnix، نوعی از تروجان بانکی Zeus، تروجان Sality، تروجان Virut و چندین نسخه از باج‌افزارها می‌پرداختند.

طبق بررسی محققان، تروجان درب پشتی Bayrob پس از 9 سال، به‌روزرسانی شده است. گفتنی است که این اقدام در ماه می انجام شده است یعنی دقیقاً همان زمانی که شرکت Proofpoint خبر از شناسایی نسخه‌های جدید بدافزار H1N1 داد.

امت کوئن، از کارمندان شرکت سیسکو در این خصوص معتقد است: «بدافزار H1N1 یک نمونه از بدافزارهایی است که در گذر زمان، تکمیل و به‌روزرسانی می‌شوند و به دلیل انواع بدافزاری که می‌تواند با خود همراه داشته باشد همواره خطری برای سازمان‌ها محسوب می‌شود. میزان مبهم‌سازی در پرونده بایری، نشان‌دهنده این است که نویسندگان این بدافزارها چقدر آماده هستند تا از کد اصلی خود محافظت کنند. انواع مختلفی از بدافزارها هستند که این میزان پیچیدگی را دارند و این چالشی بزرگ برای تحلیل‌گران است.»

اخبار تحلیلی

استفاده از حالت امن ویندوز برای نفوذ

محقق امنیتی، دوران نعیم حمله‌ای را شناسایی کرده که به نفوذگران کمک می‌کند از حالت امن ویندوز ۱۰ برای ربودن جزئیات ورود سوءاستفاده کند. به گفته این محقق، نفوذگران برای بهره‌برداری از این روش باید به یک رایانه دسترسی داشته باشند تا بتوانند ماشین مذکور را در حالت امن راه‌اندازی مجدد کنند. بدین ترتیب می‌توانند از کنترل‌های امنیتی کمتر در این محیط در جهت هدف تعیین شده استفاده کنند.

هنگامی‌که دستگاه در حالت امن قرار گیرد، می‌توان جزئیات ورود را دزدید و یا از سایر روش‌های pass-the-hash- برای نفوذ به سایر ماشین‌های شبکه شده بهره برد. برای اینکه صفحه‌ی غیرواقعی ورود را شبیه به یک صفحه راه‌اندازی عادی نشان داد و حالت امن را مخفی نگه‌داشت می‌توان از روش COM object استفاده کرد. کاربرانی که اطلاعات ورود خود را وارد می‌کنند، گمان می‌کنند که یک راه‌اندازی مجدد ساده، اطلاعات ورود را در اختیار مهاجمان قرار داده است.

نعیم بیان می‌کند: «هنگامی‌که مهاجمان از این محیط عبور کرده و دسترسی مدیریتی محلی را بر روی ماشین ویندوزی به دست می‌آورند، می‌توانند برای عبور و دست‌کاری معیارهای امنیتی نقطه‌ی انتهایی حالت امن را از راه دور فعال کنند. در حالت امن، مهاجمان می‌توانند برای به دست آوردن اطلاعات، آزادانه ابزارها را اجرا کرده و سپس، در حالی‌که ناشناس باقی می‌مانند به سامانه‌های متصل شده انتقال یابند. علی رغم وجود ماژول امن مجازی مایکروسافت، این بهره‌برداری در ویندوز 10 نیز انجام می‌شود.»

مایکروسافت مشکل بردار حمله را حل نمی‌کند زیرا اجرای این حمله مستلزم دسترسی نفوذگران به یک دستگاه ویندوزی است.

نعیم ضمن اشاره به تحقیق Fireeye که می‌گوید سال گذشته بیشتر مؤسسات سابقه‌ی فیشینگ‌های هدف‌گذاری شده را داشته‌اند، می‌گوید که دسترسی به حداقل یک دستگاه ویندوز در یک سازمان کار ساده‌ای است.

ورود به حالت امن از اعمال برخی کنترل‌های امنیتی نظیر ماژول امنیتی مجازی در ماشین میزبان جلوگیری می‌کند. این ماژول خود مسئول محدود کردن توانایی مهاجمان برای به‌کارگیری ابزارها و سرقت درهم‌سازی کلمه‌های عبور است.

نعیم می‌گوید: «الگوی ضبط اطلاعات و انتقال پس از آن، می‌تواند چندین بار توسط یک مهاجم تا حصول نهایی بهره‌برداری دامنه انجام شود.»

مهاجمان می‌توانند تا زمانی‌که قربانی، دستگاه خود را راه‌اندازی مجدد کند منتظر بمانند یا با نمایش یک هشدار، به قربانی تلقین کنند که راه‌اندازی مجدد دستگاه ضروری است.

در بررسی‌های آزمایشگاهی هنگامی‌که ضدویروس‌های

Avira ، *McAfee*، *Trend Micro*، *Microsoft*، در حالت راه‌اندازی امن غیرفعال شدند، *Mimikatz* که یک ابزار پس از بهره‌برداری است، ناشناس باقی ماند. نعیم به مدیران پیشنهاد می‌کند با تغییر منظم جزئیات ورود به مقابله با حملات *pass-the-hash* پرداخته، برای مدیران محلی حداقل سطوح اختیارات را در نظر گرفته و ابزارهای امنیتی را استفاده کنند که توانایی اجرا در حالت امن را نیز دارند.

اخبار تحلیلی

نویسنده‌ی LuaBot می‌گوید که بدافزار او خطرناک نیست!

دو هفته پیش یک محقق حوزه امنیت با نام MalwareMustDie با یک تروجان لینوکسی مواجه شد که بنا به گفته‌ی او اولین بدافزار لینوکسی بود که به زبان Lua نوشته شده بود.

آنالیز معکوس کدهای بدافزار، ثابت کرد که این تروجان معماری اینترنت اشیاء را هدف قرار داده است و این قابلیت را دارد که حملات منع سرویس توزیع‌شده را اجرا کند. همچنین دور زدن حفاظت‌های تعبیه‌شده توسط شرکت‌هایی مثل Sucuri و تولیدکننده‌های امنیت وب آمریکا را عملیاتی کند.

در کد منبع LuaBot نویسنده‌ی بدافزار پیامی از خود بجا گذاشته است با این محتوا: «سلام. بررسی‌های معکوس خوبی داشته باشید! شما می‌توانید به من ایمیل بزنید.» و آدرس ایمیل خود را نوشته است.

نویسنده‌ی LoaBot به تعدادی سوال پاسخ داده است!

یک محقق امنیت فرانسوی با نام x0rz با نویسنده‌ی بدافزار ارتباط برقرار کرده و از او سوالاتی را پرسیده است. این پاسخ‌ها بطور برخط منتشر شده است.

در این مصاحبه‌ی کوتاه، مهاجم گفته که برای انجمن infosec کار نمی‌کند و همچنین کارمند وابسته به هیچ گروه مجرم در فضای مجازی نیست.

او خودش را «هیچ‌کس» معرفی کرده و گفته است که بدافزار او خطرناک نیست. او مبنای این ارزیابی را عملکرد بدافزار خود عنوان می‌کند بطوری‌که این بدافزار اعتبارنامه‌های ورود مسیریاب‌ها را به سرقت نمی‌برد.

نویسنده‌ی LuaBot می‌گوید که این بدافزار برای حملات منع سرویس توزیع‌شده بکار نمی‌رود!

نویسنده‌ی LuaBot می‌گوید که سال‌ها بر روی این بدافزار کار کرده است و چیزی که ابتدا برای سرگرمی شروع شده بود الان تبدیل به منبع سود شده است.

او از گفتن فعالیتی که این بدافزار برای او سودآوری می‌کند، امتناع کرده است ولی می‌گوید که این بدافزار هیچ سرویس منع سرویس توزیع‌شده‌ای را همانند vDos kids ارائه نمی‌دهد. علاوه بر این او عنوان کرد که با اشخاص خصوصی کار می‌کند و توسط بانک‌ها یا دولت تامین نمی‌شود.

آنالیزها چیزهای جالبی را فاش می‌کند.

این مهاجم عنوان می‌کند که روز-صفرم مخصوص به خود را دارد که از آن برای آلوده کردن تجهیزات استفاده می‌کند. یک محقق امنیتی برزیلی که بدافزار را دیده است، می‌گوید به نظر می‌رسد که این کد، مسیریاب‌های ARRIS را هدف قرار داده است. این همان محققی است که سال پیش نیز 3 درب پشتی را در مسیریاب‌های ARRIS افشاء کرد که 600 هزار مودم متصل برخط را تحت تاثیر

قرار می‌داد.

برناردو رودریگز، محقق برزیلی عنوان می‌کند: «اگر همین امروز پرس‌وجوهای یکسانی انجام شود، ما شاهد خواهیم بود که تعداد تجهیزات در معرض خطر به تقریبا 35000 کاهش یافته است.»

این محقق همچنین عنوان می‌کند که در وهله‌ی اول آلوده‌شدن به این بدافزار، LuaBot از قواعد دیواره‌ی آتش برای مسدود کردن دسترسی از ارتباطات خارجی استفاده می‌کند که این یک ویژگی خود-محافظتی صریح است. با این وجود، این بدافزار ساز و کار پایداری از طریق بوت را ندارد و آغاز به کار مجدد مسیریاب، این بدافزار را از آن وسیله حذف می‌کند.

در زمان نگارش این خبر، هیچ حمله‌ای گزارش نشده است که مستعد آلودگی به این بدافزار باشد و برخلاف وجود عملیات سیل‌آسای HTTP برای حملات منع سرویس توزیع‌شده، این بدافزار و اهداف آن به صورت یک راز باقی مانده است.

Expert Bulletin News

Information Communication Technology

2th year 2016 | Weekly bulletin

اخبار فناوری اطلاعات و ارتباطات

هفته نامه | شماره هفتاد و سوم | سال دوم | ۶۵ صفحه

خبرنامه هفتگی کارشناسی

مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج