سراج

۲۶ فروردین ۱۳۹۶

شماره ۱۰۸

اخبار فناوری اطلاعات و ارتباطات

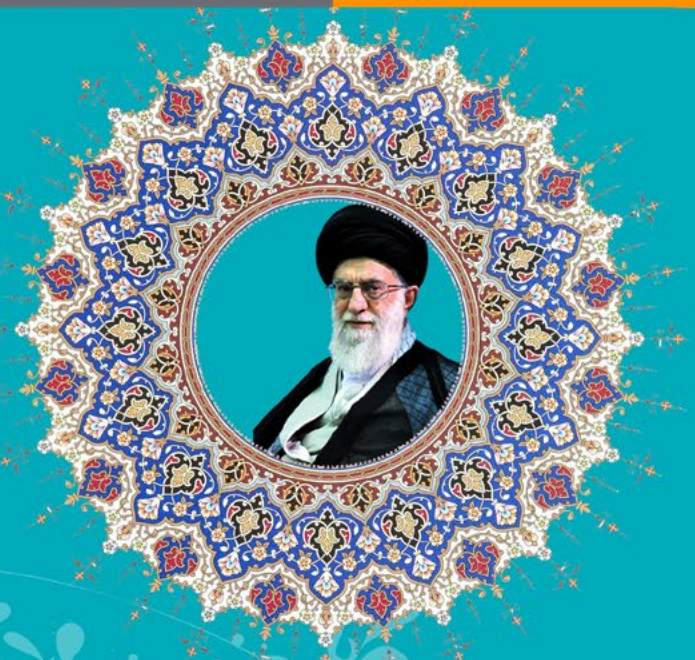
مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج

هفته نامه | شماره صد و هشتم | سال سوم | ۳۷ صفحه

در این شماره می‌خوانید:

بسم الله الرحمن الرحیم

آگاهی و بصیرت



یک وقتی می گفتیم ده ها رادیو؛ امروز مسئلهٔ هزارهاست؛ رادیو هست؛ تلویزیون هست؛ این وسایل اینترنتی هست – مرتباً القای بن بست، القای بحران [و] القای سیاه بودن وضعیت می شود؛ هر مقداری که بگیرد؛ هر مقداری که مستمع و شنونده پیدا بکند و باورپذیر باشد برای آنها. دارند در این زمینه کار می کنند. این، یکی از خطوط کاری دشمن است.

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

ابزار رمزگشایی برای باج‌افزار Bart توسط بیت‌دیفندر منتشر شد

ظهور باج‌افزارها بدین معنی است که تعداد زیادی از قربانیان، پرونده‌های خود را از دست خواهند داد و یا پول زیادی را در جیب مهاجمان سایبری خواهند ریخت. با این حال، کاربرانی که سامانه‌ی آن‌ها به باج‌افزار Bart آلوده شده، دیگر لازم نیست نگران باشند چرا که شرکت بیت‌دیفندر ابزار رمزگشایی برای این بدافزار را منتشر کرده است.

باج‌افزار Bart برای اولین بار در ژوئیه‌ی سال 2016 میلادی مورد بررسی قرار گرفت ولی تاکنون راه‌حلی برای بازیابی پرونده‌هایی که بوسیله‌ی این بدافزار رمزنگاری شده بود، وجود نداشت. با استفاده از ابزار رمزگشایی که شرکت بیت‌دیفندر منتشر کرده، می‌توان پرونده‌های رمزنگاری‌شده با پسوندهای مختلف را بازیابی کرد. بیت‌دیفندر اعلام کرد این ابزار با همکاری این شرکت با یوروپل و پلیس رومانیا طراحی و توسعه داده شده است.

باج‌افزار Bart چگونه کار می‌کند؟

باج‌افزار Bart متمایز از سایر خانواده‌های باج‌افزاری است چرا که می‌تواند پرونده‌های قربانی را بدون نیاز به اتصال اینترنت، رمزنگاری کند. با این‌حال در فرآیند رمزگشایی به اتصال اینترنت نیاز است تا مهاجم به کارگزار دستور و کنترل متصل شده، بیت‌کوین‌های پرداختی ارسال شود و در نهایت کارگزارِ مهاجم، کلیدهای رمزگشایی را در اختیار قربانی قرار دهد.

این بدافزار اگر زبان رایانه، یکی از زبان‌های روسی، بلاروس و اوکراینی باشد، عملیات خود را ادامه نمی‌دهد و این می‌تواند نشان دهد که بدافزار توسط یک نفوذگر روسی نوشته شده است. این بدافزار نقاط بازیابی سامانه را حذف کرده، با استفاده از اطلاعات موجود بر روی ماشین به تولید کلیدهای رمزنگاری می‌پردازد، پرونده‌ها را شمارش کرده و تمامی آن‌ها را با استفاده از این کلید رمزنگاری می‌کند.

در ادامه نیز پیش از نمایش پیغام باج‌خواهی و هدایت کاربر به سمت یک وب‌گاه .onion، تمامی کلیدهای مورد استفاده برای رمزنگاری پرونده‌ها را با یک کلید اصلی رمزنگاری می‌کند. محققان امنیتی معتقدند توسعه‌دهنده‌ی باج‌افزار Bart همان توسعه‌دهنده‌ی باج‌افزارهای Dridex و Locky است که از هرزنامه‌ها برای توزیع بدافزار خود استفاده می‌کنند.

اخبار عمومی

باج‌افزاری که از شما می‌خواهد بازی رایانه‌ای انجام داده و به امتیاز بالا برسید

این حقیقت که ظهور باج‌افزارها رفته‌رفته بیشتر و بیشتر می‌شود چیز جدیدی نیست ولی اینک یک باج‌افزار جدید ظاهر شده که از قربانی می‌خواهد تا یک بازی انجام داده و در آن به امتیازات بالا برسد تا مهاجم پرونده‌های او را برگرداند.

به گفته‌ی محققان امنیتی، باج‌افزار rensenWare از قربانیان می‌خواهد تا در یک بازی بسیار سخت رایانه‌ای به امتیاز بالایی دست پیدا کنند تا پرونده‌های آن‌ها را رمزگشایی کند. معمولاً نویسندگان باج‌افزار برای بازیابی پرونده‌های رمزنگاری‌شده از قربانی باج در قالب بیت‌کوین درخواست می‌کنند.

این باج‌افزار چه می‌خواهد؟ این بدافزار در ابتدای امر تمامی پرونده‌های موسیقی و تصویری قربانی را رمزنگاری می‌کند. در ادامه از قربانیان می‌خواهد تا در یک بازی رایانه‌ای به امتیاز 0.2 میلیارد برسند هرچند این امتیاز خیلی مقدار بالایی نیست ولی برای کسی که بازیکن حرفه‌ای نباشد، سخت است.

هرچند مشخص است که این باج‌افزار یک تهدید جدی نبوده و بیشتر به یک شوخی شبیه است. نویسنده‌ی این باج‌افزار پس از اینکه بدافزار او به‌طور عمومی منتشر شد، در توییتر پستی را برای معذرت‌خواهی از کاربران منتشر کرد.

نویسنده‌ی این باج‌افزار که معمولاً به زبان کره‌ای در توییتر پست منتشر می‌کند گفت: «اول از همه، از تمامی کسانی که توسط این بدافزار شوکه و یا اذیت شدند عذرخواهی می‌کنم. من صرفاً این باج‌افزار را برای شوخی و خندیدن توسعه دادم. من کد منبع آن را در وب منتشر کردم و زمان انتشار آن، نقطه‌ی آغاز تراژدی بوده است.»

این نفوذگر ادعا می‌کند که حذف منطق رمزنگاری و رمزگشایی در کد منبع پیش از انتشار ایده‌ی بسیار خوبی بوده است ولی او در این راه با شکست مواجه شده است. نویسنده‌ی بدافزار معتقد است که مردم حق دارند که او را بخاطر انتشار کد این بدافزار سرزنش کنند.

نویسنده‌ی بدافزار در توضیحات خود گفت: «من کد منبع باج‌افزار rensenWare را بر روی گیت‌هاب منتشر کردم تا اگر ممکن است این ابزار به کسانی که تحت تأثیر قرار گرفته‌اند کمکی کرده باشد. من دوباره از همگان عذرخواهی می‌کنم. من واقعا متأسفم.»

در حال حاضر در کد منبع این بدافزار، بخش‌های رمزنگاری و رمزگشایی حذف شده است ولی حذف شدن این توابع بر روی گیت‌هاب، به این معنی نیست که بدافزار به‌طور کامل از روی اینترنت حذف شده باشد.

اخبار عمومی

رکوردهای جستجو در Ask.com به‌طور عمومی افشاء شده است

صفحه‌ی وضعیت کارگزار آپاچی مربوط به وب‌گاه Ask.com در دسترس عموم قرار دارد و همه می‌توانند مشاهده کنند که چه کسی چه چیزی را جستجو کرده است. هرکس نگاهی به این صفحه بیندازد می‌تواند پرس‌وجوها و عملیاتی که توسط افراد بر روی این کارگزار انجام شده را مشاهده کند.

این مسئله امروز صبح توسط محقق امنیتی با نام پل شاپیرو کشف شده و حتی بعد از گذشت ساعت‌ها از انتشار این خبر، Ask.com اطلاعات این کارگزار را از دید کاربران مخفی نکرده است.

هنوز مشخص نیست این صفحه از چه زمانی به‌طور عمومی باز بوده است و باتوجه به بی‌توجهی این شرکت، تا چه زمانی این‌طور در معرض دید عموم باقی خواهد ماند. این صفحه 3 روز قبل مجدداً راه‌اندازی شده و به نظر می‌رسد این راه‌اندازی مجدد، این کارگزار را در معرض دید عموم قرار داده است.

این موضوع یک تهدید امنیتی نیست

در حالی که بر روی این صفحه به‌طور کامل می‌توان مشاهده کرد که چه مطالبی جستجو شده است ولی خوشبختانه آدرس IP افرادی که این موارد را جستجو کرده‌اند در این صفحه نمایش داده نمی‌شود. در حقیقت تمامی آدرس‌های IP که فهرست شده، آدرس‌های داخلی هستند و به‌عبارتی می‌توان گفت آدرس‌ها متعلق به دیواره‌ی آتش Ask.com هستند.

این نقض داده نگران‌کننده است ولی نگرانی خیلی زیاد نیست چرا که آدرس‌های IP کاربران در معرض دید عموم قرار ندارد. به همین دلیل تمامی اطلاعاتی که بر روی این کارگزار افشاء شده یک تهدید امنیتی محسوب نمی‌شود. هرچند افشای چنین اطلاعاتی به‌طوری که همه بتوانند آن را مشاهده کنند خیلی معمول نیست. امیدواریم این مشکل هرچه سریع‌تر برطرف شده و Ask.com در مورد آن اظهارنظر کند. در حال حاضر شما می‌توانید این صفحه را مجدداً بارگذاری کرده و جستجوهای جدید را مشاهده کنید.

فصل دوم

مدیریت امنیت

مدیریت امنیت

دادگاه کانادا قبول وثیقه از نفوذگر یاهو را رد کرد

دادگاهی در کانادا روز سه‌شنبه قبول وثیقه برای آزادی نفوذگری که به نفوذ سایبری عظیم علیه یاهو متهم شده را رد کرد. این فرد منتظر درخواست استرداد از طرف آمریکا است. کریم باراتو 22 ساله اهل قزاقستان، به اتهام نفوذ، جاسوسی تجاری و دیگر جرائم در ماه مارس با حکم دادگاه آمریکا دستگیر شده است.

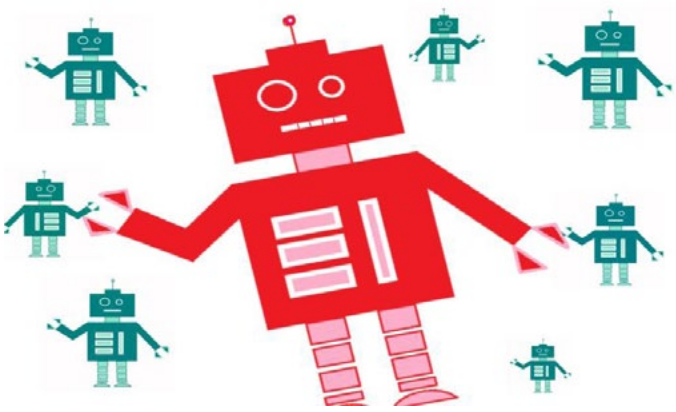
وکیل باراتو اعلام کرد آن‌ها قصد دارند به حکم استرداد باراتو به آمریکا اعتراض کنند. فرآیند بازرسی اوایل ماه ژوئن آغاز شده و روند تصمیم‌گیری برای استرداد او انتظار می‌رود 3 سال به طول انجامد. مقامات رسمی آمریکا معتقدند دیپلمات‌های جاسوس روسیه، باراتو و یک نفوذگر دیگر را برای انجام نفوذ و جاسوسی از حساب‌های یاهو در بازه‌ی سال‌های 2014 تا 2016 میلادی استخدام کرده‌اند.

در نقض داده‌ای که گریبان‌گیر شرکت یاهو شد، اطلاعات 500 میلیون حساب کاربری افشاء شده بود و این اتفاق در نوع خود، بزرگ‌ترین نقض داده‌ی تاریخ محسوب می‌شود. اهداف این نفوذ شامل مقامات روسیه و آمریکا، امنیت سایبری، پرسنل نظامی و دیپلماتیک، روزنامه‌نگاران، شرکت‌ها و مؤسسات مالی بوده است.

وکیل باراتو برای او حصر خانگی را درخواست کرده که دادگاه با این موضوع موافقت نکرده است. دادستان اعلام کرد که باراتو متهم به جاسوسی از دولت‌های خارجی است و در ضمن یکی از هم‌دستان او موفق شده به روسیه فرار کند.

مدیریت امنیت

تلاش برای از کار انداختن باتنت Kelihos پس از دستگیری نفوذگر روسی در اسپانیا



اینک که یک نفوذگر روسی با نام پیوتر لواشو با نام مستعار Severa در اسپانیا دستگیر شده است، مقامات رسمی آمریکا در تلاش هستند تا باتنت‌های این نفوذگر را که سالانه برای ارسال میلیاردها هرزنامه استفاده می‌شود، از کار بیندازند.

براساس بیانیه‌ی وزارت دادگستری آمریکا، تلاش‌ها برای از کار انداختن باتنت Kelihos آغاز شده است. باتنت Kelihos یک شبکه‌ی جهانی از رایانه‌های ویندوزی است که آلوده شده و برای ارسال هرزنامه‌ها برای تبلیغ داروها و محصولات قاچاق مورد استفاده قرار می‌گیرند. هرچند این پویش تلاش خود برای بدست آوردن گذرواژه و آلوده کردن سامانه‌ها به بدافزار را ادامه می‌دهد.

این بیانیه پس از آن منتشر شد که خبر دستگیری لواشو در کل جهان پخش شد. گفته می‌شود Severa حداقل از سال 2010 میلادی به استفاده از باتنت هرزنامه‌ای مشغول بوده است. به گزارش محققان امنیتی، او در حال حاضر در بین 10 ارسال‌کننده‌ی برتر هرزنامه در جهان در مقام هفتم قرار دارد.

مقامات آمریکایی افزودند از کار انداختن باتنت Kelihos نتیجه‌ی همکاری بین کارشناسان شرکت‌های خصوصی و مراجع قانونی بوده که از روش‌های خلاقانه‌ی فنی و قانونی استفاده کرده‌اند. براساس گزارش FBI عملیات برای از کار انداختن باتنت Khelios از تاریخ 19 فروردین ماه با مسدود کردن دامنه‌های مرتبط با این باتنت آغاز شده تا جلوی آلودگی‌های بیشتر گرفته شود.

کارشناسان امنیتی می‌گویند: «حکم لازم برای هدایت رایانه‌های آلوده به باتنت Kelihos به سمت یک کارگزار جایگزین توسط مقامات قانونی صادر شده است تا در ادامه با استفاده از ترافیکی که این رایانه‌ها به سمت کارگزار مورد نظر ارسال می‌کنند، آدرس IP آن‌ها بدست آید. این کار مقامات قانونی را قادر می‌سازد تا آدرس‌های IP را در اختیار شرکت‌ها امنیتی و ارائه‌دهندگان سرویس اینترنت قرار دهند.» هرچند مدت زمان کوتاهی از این مسئله می‌گذرد ولی احتمالاً این باتنت به‌طور کامل از کار افتاده است.

مدیریت امنیت

شرکت پرداخت وام با نام Wonga در انگلستان دچار نقض داده‌ی بزرگی شده است

شرکت پرداخت وام در انگلستان با نام Wonga به مشتریان خود اطلاع داد که احتمالاً در یک حمله‌ی سایبری، بخشی از داده‌های شخصی و مالی این شرکت به سرقت رفته است. براساس گفته‌های این شرکت، نفوذگران توانسته‌اند به نام، آدرس رایانامه، آدرس فیزیکی، شماره تماس، اطلاعات کارت اعتباری و کارت بانکی کاربران دست یابند. بررسی‌های این شرکت در حال انجام است.

شرکت Wonga اعلام کرده هنوز شواهدی مبنی بر سرقت گذرواژه‌های کاربران وجود ندارد ولی کاربرانی که نگران هستند، برای اطمینان می‌توانند گذرواژه‌ی خود را تغییر دهند. به مشتریانی که تحت تأثیر قرار گرفته‌اند اطلاع‌رسانی شده است.

روزنامه‌ی گاردین گزارش داد که در این حادثه نزدیک به 270 هزار مشتری فعلی و سابق ساکن در انگلستان و لهستان تحت تأثیر قرار گرفته‌اند. تقریباً 245 هزار مورد از قربانیان این حادثه اهل انگلستان هستند.

هرچند در این نفوذ، کل اطلاعات کارت‌های بانکی به سرقت نرفته است ولی Wonga اعلام کرده به مؤسسات مالی اطلاع‌رسانی کرده و به مشتریان گفته شده برای بررسی هرگونه رفتار مشکوک در حساب‌ها با بانک‌های خود در ارتباط باشند.

این حادثه یکی از بزرگ‌ترین نقض داده‌هایی است که یک شرکت انگلستانی تجربه کرده است. دفتر کمیساریای این کشور، گروهی را برای بررسی این حادثه راه‌اندازی کرده است و این بررسی می‌تواند برای شرکت مربوطه جریمه‌ی سنگینی در پی داشته باشد.

فصل سوم

امنیت سایبری

امنیت‌سایبری

گروه نفوذ Shadow Brokers ابزارهای نفوذ بیشتری متعلق به آژانس امنیت ملی آمریکا را منتشر کرد

آیا گروه نفوذ The Shadow Brokers را به‌خاطر دارید؟ آن‌ها دوباره برگشته‌اند. این گروه نفوذ سال گذشته مدعی شده بود بخشی از ابزارهای نفوذ متعلق به آژانس امنیت ملی آمریکا را بدست آورده که این ابزارها شامل بدافزار و بهره‌برداری از آسیب‌پذیری‌های روز-صفرم بود. اواخر سال گذشته نیز این گروه نتوانست ابزارهای سرقتی را به قیمت مورد نظر خود به فروش برساند و مجبور شد آن‌ها را به‌طور برخط منتشر کند.

روز گذشته این گروه نفوذ ابزارها و بهره‌برداری‌های جدیدی را منتشر کرده و مدعی شده متعلق به گروه نفوذ Equation است. محققان امنیتی و سایر نفوذگران معتقدند گروه Equation توسط آژانس امنیت ملی آمریکا مورد حمایت قرار می‌گیرد و این گروه در نفوذهای این سازمان اطلاعاتی نقش دارد.

علاوه بر ابزارهای نفوذ آژانس امنیت ملی که این گروه به‌طور عمومی منتشر کرده بود، یک پرونده‌ی رمزنگاری‌شده از ابزارهای دیگر نیز وجود داشت که این گروه برای در اختیار قرار دادن آن مزایده‌ای با مبلغ 1 میلیون بیت‌کوین، معادل 568 میلیون دلار برگزار کرده بود.

پس از اینکه این مزایده با شکست مواجه شد، گروه نفوذ ابزارهای خود را برای فروش مستقیم به بازارهای زیرزمینی برد و آن‌ها را در گروه‌های مختلفی از جمله بهره‌برداری و تروجان دسته‌بندی کرد. قیمت هر یک از این دسته‌ها از 1 تا 100 بیت‌کوین متغیر بود.

بالاخره گروه Shadow Brokers گذرواژه‌ی این پرونده‌ی رمزنگاری‌شده را اعلام کردند تا عموم بتوانند از این ابزارهای نفوذ متعلق به آژانس امنیت ملی استفاده کنند. گذرواژه CrDj"(;Va.*NdlnzB9M?@K2)#>deB7mN است. این گذرواژه در یک پست وبلاگی به‌طور عمومی افشاء شده است.

در این پست وبلاگی با عنوان «اصل خود را فراموش نکنید» یک نامه‌ی سرگشاده خطاب به رئیس جمهور آمریکا، دونالد ترامپ نوشته شده است و گروه نفوذ Shadow Brokers عقاید سیاسی خود را نسبت به وقایع اخیر و اقدامات دولت ترامپ از جمله حمله‌ی هوایی به سوریه بیان کرده‌اند.

یک محقق امنیتی که در توییتر با شناسه‌ی x0rz، فعالیت می‌کند پس از دریافت و رمزگشایی این پرونده‌ها، تمامی آن‌ها را در گیت‌هاب بارگذاری کرده است. در حال حاضر هنوز مشخص نیست که آیا این آخرین اسناد باقی مانده در دست این گروه بود که منتشر شده است یا گروه Shadow Brokers هنوز هم ابزارهای دیگری متعلق به آژانس امنیت ملی آمریکا را در دست دارند.

امنیت‌سایبری

جعل تراکنش بیت‌کوین برای نشان دادن پرداخت باج توسط اپل به نفوذگران iCloud

یک گروه نفوذ که اخیراً اعلام کرده بود کنترل میلیون‌ها حساب iCloud را در دست دارد و برای حذف نکردن اطلاعات این حساب‌ها از شرکت اپل باج درخواست کرده بود، روز جمعه اعلام کرد که باجِ درخواستی آن‌ها پرداخت شده است. با این‌حال یک کارشناس بیت‌کوین می‌گوید این موضوع ساختگی و جعلی است.

گروه نفوذ خانواده‌ی جرائم تُرک ماه گذشته در صدر خبرها قرار گرفته بود و اعلام کرد کنترل بیش از 700 میلیون حساب me.com، icloud.com و mac.com را در دست دارد. آن‌ها شرکت اپل را تهدید کرده بودند که اگر باج درخواستی آن‌ها را پرداخت نکند، تمامی اطلاعات این حساب‌ها را حذف خواهند کرد.

روز جمعه، این گروه نفوذ در توییتی اعلام کرد که مبلغ 480 هزار دلار را در قالب بیت‌کوین دریافت کرده است. برای اثبات این موضوع نیز یک پیوند مربوط به انجام تراکنش در کیف پول Blockchain.info را منتشر کرد. پیش از ارسال توییت در مورد پرداخت باج، گروه نفوذ در توییت دیگری اعلام کرده بود: «ما با مذاکره با شرکت اپل به توافق رسیده‌ایم.»

با این حال یک کارشناس حوزه‌ی بیت‌کوین می‌گوید، پیوندی که نفوذگران منتشر کرده‌اند مربوط به یک عملیات داخلی در خزانه‌ی بیت‌کوین است. این محقق اعلام کرد این تراکنش بخشی از فرآیند داخلی واریز پول در یک بازار بیت‌کوین کره‌ای بوده است.

شرکت اپل در مورد این مسائل هیچ اظهارنظری نکرده و قبلاً اعلام کرده هیچ‌گونه نقض داده‌ای در سرویس‌های این شرکت رخ نداده است. اپل گفته است گواهی‌نامه‌هایی که در اختیار نفوذگران قرار گرفته به احتمال زیاد، از نقض داده در سرویس‌های دیگر بدست آمده است. محققان امنیتی نیز گفته‌ی اپل را تأیید کرده‌اند و معتقدند این گروه نفوذ در ادعای خود اغراق کرده است.

امنیت‌سایبری

یک نفوذگر روسی به اتهام جرائم سایبری متعدد در اسپانیا دستگیر شد

یک برنامه‌نویس روس در اسپانیا به اتهام شرکت در چند نفوذ سایبری دستگیر شده است. گفته می‌شود این دستگیری مربوط به نفوذهایی است که پاییز سال گذشته در جریان انتخابات ریاست جمهوری آمریکا رخ داده بود. به گزارش خبرگزاری‌های اسپانیا، پیوتر لواشو در 18 فروردین ماه در بارسلونا دستگیر شد و در حال حاضر در بازداشت به سر می‌برد.

یکی از مراجع قانونی اسپانیا به خبرگزاری‌ها گزارش داده که لواشو از طرف آمریکا مورد استرداد قرار گرفته ولی این موضوع هنوز در دادگاه اسپانیا در حال بررسی است.

یک وب‌گاه خبری در اسپانیا در پستی نوشته است، دستور دستگیری لواشو توسط دولت آمریکا صادر شده است و دلیل آن نفوذ به رایانامه‌های حزب دموکرات در جریان انتخابات ریاست جمهوری آمریکا بوده است. این موضوع توسط همسر لواشو نیز تأیید شده است.

با این حال منابع رسمی، این مسئله را رد کرده و می‌گویند دستگیری او به‌خاطر نفوذهایی در مقیاس بالا بوده و نه چیزی بیشتر. در این وب‌گاه اشاره شده شرایط فعلی هیچ ربطی به دخالت روسیه در انتخابات ریاست جمهوری آمریکا ندارد.

محققان امنیتی جزئیات زیادی درباره‌ی لواشو منتشر کرده‌اند. او در جامعه‌ی نفوذگران بیشتر با نام مستعار Severa شناخته می‌شود. برایان کربس، محقق امنیتی مشهور می‌نویسد او یکی از ارکان اساسی ارسال هرزنامه در فضای مجازی است و اوست که نویسندگان بدافزار را به پویش‌های هرزنامه‌ای برای توزیع متصل می‌کند.

برایان کربس برای لواشو فهرست طولانی از جرائم سایبری را ارائه کرده است. به‌عنوان مثال، او در بین 10 ارسال‌کننده‌ی برتر هرزنامه در جهان، در مقام هفتم قرار دارد. او یکی از عوامل اصلی باتنت هرزنامه‌ای Waladec بوده که ده‌ها هزار رایانه را با ارسال 1.5 میلیارد هرزنامه در هر روز آلوده کرده است.

امنیت‌سایبری

انتشار چارچوب Grasshopper متعلق به سازمان سیا توسط ویکی‌لیکس

در ادامه‌ی اسناد Vault 7 که ویکی‌لیکس از قابلیت‌های نفوذ سازمان سیا افشاء کرده است، روز گذشته، 27 سند جدید نیز از بهره‌برداری‌های مورد استفاده توسط سازمان سیا منتشر شده است.

این ابزار جدید با نام Grasshopper یک چارچوب خط فرمان برای توسعه‌ی بدافزارهای ویژه است که توسط سازمان سیا برای هدف قرار دادن سامانه عامل ویندوز شرکت مایکروسافت طراحی شده تا راه‌حل‌های ضدبدافزاری را دور بزنند. ویکی‌لیکس ادعا می‌کند تمامی اسنادی که افشاء شده به‌نوعی کتابچه‌ی راهنما محسوب شده و تحت عنوان «محرمانه» برچسب‌گذاری شده‌اند تا تنها اعضای این سازمان بتوانند به آن دسترسی داشته باشند.

Grasshopper: چارچوب توسعه‌ی بدافزار ویژه

براساس اسناد منتشرشده، چارچوب Grasshopper به اعضای سازمان سیا اجازه می‌داد تا باتوجه به جزئیات فنی سامانه عامل و ضدبدافزار مورد نظر، بدافزارهای مخصوص را توسعه دهند. این چارچوب در ادامه برای حمله به سامانه‌ی مورد نظر، مؤلفه‌های مختلف را کنار هم قرار می‌دهد و در نهایت یک پرونده‌ی نصب را ارائه می‌کند که اعضای سازمان سیا می‌توانند آن را بر روی سامانه‌ی هدف نصب و اجرا کنند.

ویکی‌لیکس مدعی است بدافزارهایی که توسط چارچوب Grasshopper ایجاد می‌شوند طوری طراحی شده‌اند تا راه‌حل‌های امنیتی ارائه‌شده توسط شرکت‌های بزرگی مانند آزمایشگاه کسپرسکی، سیمانتک و مایکروسافت را دور بزنند.

به گزارش ویکی‌لیکس سازمان سیا نه تنها این چارچوب را طوری طراحی کرده که برای استفاده در اهداف جاسوسی، آسان و کاربرپسند باشد بلکه طراحی آن را طوری در نظر گرفته تا در سامانه‌ی آلوده‌ی ویندوز به سازوکار ماندگاری نیز دست یابد. برای رسیدن به ماندگاری نیز از روش‌های معروف و شناخته‌شده در فضای سایبری استفاده کرده است.

به‌طور مثال این چارچوب قادر است روش ماندگاری موجود در بدافزار Carberp را پیاده‌سازی کند. این بدافزار یک روت‌کیت است که توسط نفوذگران روسی توسعه داده شده است. هنوز به‌طور کامل مشخص نیست که سازمان سیا اخیراً چگونه از ابزارهای ذکرشده در این اسناد استفاده کرده است ولی ویکی‌لیکس می‌گوید این ابزارها در بازه‌ی سال‌های 2012 تا 2015 میلادی مورد استفاده قرار گرفته است.

چندی پیش نیز شاهد بودیم که ویکی‌لیکس چارچوب Marble را منتشر کرد که برای سخت‌تر کردن فرآیند جرم‌شناسی در حملات سازمان سیا مورد استفاده قرار می‌گرفت. این چارچوب به مبهم‌سازی بدافزار می‌پرداخت و فرآیند ردیابی آن را مشکل می‌ساخت.

امنیت‌سایبری

ابزارهای نفوذ سازمان سیا با حملات جاسوسی علیه ۱۶ کشور مرتبط است

به گزارش سیمانتک، ابزارهای جاسوسی و نفوذ متعلق به سازمان سیا که توسط ویکی‌لیکس افشاء شده است، تقریباً 40 نهاد را در 16 کشور هدف قرار داده است. در گزارشی که سیمانتک روز دوشنبه منتشر کرد، این ابزارها اشتراک زیادی با روش‌هایی دارد که توسط یک گروه جاسوسی با نام Longhorn مورد استفاده قرار می‌گیرد. این گروه جاسوسی حداقل از سال 2011 میلادی فعال بوده و با استفاده از تروجان و آسیب‌پذیری‌های ناشناخته به اهداف خود حمله می‌کرده است.

سیمانتک در مورد سازمان‌هایی که هدف این حملات جاسوسی قرار داشتند، اطلاعات دقیقی ارائه نکرد ولی گفته می‌شود این بخش‌ها، سازمان‌های دولتی و صنایع در حوزه‌ی مالی، مخابراتی، فناوری اطلاعات و هوافضا هستند. رایانه‌های قربانی در خاورمیانه، اروپا، آسیا و آفریقا واقع شده‌اند و در یک مورد نیز سازمان هدف در آمریکا قرار دارد هرچند که سازمان سیا عملیات نظارتی در این کشور را رد کرده است. سیمانتک گفت: «به دنبال این عملیات جاسوسی، یک رایانه در آمریکا نیز آلوده شده است ولی این آلودگی پس از ساعاتی حذف شد و به نظر می‌رسد این دستگاه به‌طور ناخواسته آلوده شده است.»

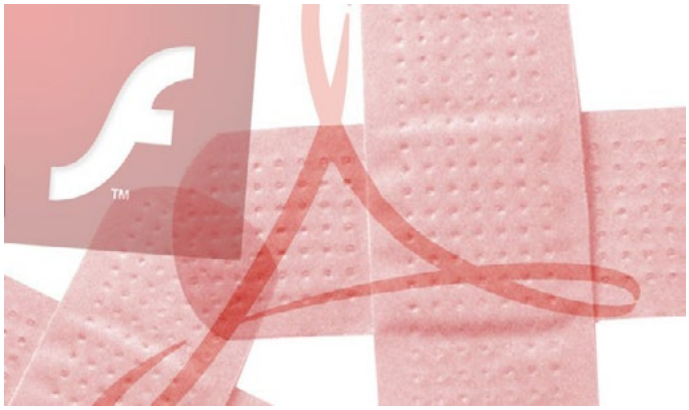
سازمان سیا در مورد صحت اسنادی که ویکی‌لیکس منتشر کرده هیچ اظهارنظری نکرده است. روز دوشنبه سیمانتک اعلام کرد شکی نیست که بین گروه جاسوسی Longhorn و ابزارهای نفوذ سازمان سیا که ویکی‌لیکس منتشر کرده، ارتباطی وجود دارد. این شرکت امنیتی اعلام کرد Longhorn از 4 بدافزار در حملات خود استفاده می‌کند که 2 مورد از آن‌ها دقیقاً همان چیزی است که در اسناد ویکی‌لیکس تشریح شده است. به‌عنوان مثال در اسنادی که ویکی‌لیکس منتشر کرده یک بدافزار با نام Fluxwire و تاریخ تغییراتی که در آن اعمال شده، منتشر شده است. سیمانتک اعلام کرده با نظارتی که بر روی عملیات گروه Longhorn داشته، این تاریخ‌ها با زمان انتشار نسخه‌ی جدید از تروجان این گروه مطابقت دارد. یکی دیگر از بدافزارهای موجود در اسناد سازمان سیا نیز با بدافزار مورد استفاده توسط گروه Longhorn مطابقت دارد که برای ایجاد یک دربِ پشتی در سامانه‌های ویندوزی مورد استفاده قرار می‌گیرد. سیمانتک می‌گوید برخی شواهد نشان می‌دهد که سابقه‌ی گروه Longhorn به سال 2007 میلادی برمی‌گردد. با این حال پیش از افشای اسناد سازمان سیا توسط ویکی‌لیکس، سیمانتک به این نتیجه رسیده بود که این گروه جاسوسی دارای منابع کافی بوده و به اطلاعات زیادی دسترسی دارند و احتمالاً انگلیسی زبان هستند. ویکی‌لیکس هیچ یک از ابزارهای مورد استفاده توسط سازمان سیا را منتشر نکرده و اسنادی که ارائه داده در حد یک کتابچه‌ی راهنما هستند. محققان امنیتی معتقدند این اسناد نمی‌توانند به شرکت‌های امنیتی و یا دولت‌های خارجی در کشف روش‌های سازمان سیا هیچ کمکی بکنند.

فصل چهارم

اخبار فنی

اخبار فنی

شرکت ادوبی آسیب‌پذیری‌های موجود در محصولات خود را وصله کرد



شرکت ادوبی روز سه‌شنبه به‌روزرسانی امنیتی را برای محصولات خود منتشر کرد که در آن به‌طور کلی 59 آسیب‌پذیری وصله شده بود. از جمله آسیب‌پذیری‌هایی که این هفته وصله شده‌اند، می‌توان اشکالاتی که در مسابقه‌ی Pwn2Own امسال افشاء شد را نام برد.

اکثر آسیب‌پذیری‌ها و یا اگر بخواهیم دقیق‌تر بگوییم، 47 مورد از آسیب‌پذیری‌ها بر روی نسخه‌ی ویندوز و مک ادوبی آکروبات و ادوبی ریدر وصله شده است. این آسیب‌پذیری‌ها جدی بوده و مربوط به خرابی حافظه هستند که بهره‌برداری موفق از آن‌ها به مهاجم اجازه‌ی اجرای کد دلخواه را داده و منجر به نشت حافظه می‌شود. در ادوبی فلش‌پلیر نیز 7 آسیب‌پذیری حیاتی وصله شده است. این آسیب‌پذیری‌ها، استفاده پس از آزادسازی و خرابی حافظه بودند که در صورت بهره‌برداری، به مهاجم اجازه‌ی اجرای کد بر روی سامانه‌ی آسیب‌پذیر را می‌دادند. بسیاری از آسیب‌پذیری‌ها توسط محققان امنیتی ترندمیکرو به شرکت ادوبی گزارش شده است که تعدادی از آن‌ها نیز در مسابقه‌ی Pwn2Own افشاء شده بود.

شرکت ادوبی همچنین آسیب‌پذیری‌هایی را در محصولات دیگر مانند فتوشاپ سی‌سی نسخه‌ی مک و ویندوز، Campaign و Creative Cloud Desktop Application در ویندوز وصله کرده است. این شرکت اعلام کرد بهره‌برداری از این آسیب‌پذیری‌ها در دنیای واقعی را مشاهده نکرده است.

یک آسیب‌پذیری روز-صفرم دارای شناسه‌ی CVE-2017-0199 است و یک اشکال مربوط به آفیس و وردپد است که برای توزیع بدافزارهایی مانند Dridex، WingBird، Latentbot و Godzilla مورد بهره‌برداری قرار می‌گیرد. یک آسیب‌پذیری دیگر با شناسه‌ی CVE-2017-0210 مربوط به ارتقاء امتیاز است که در اینترنت اکسپلورر وجود دارد.

یک آسیب‌پذیری روز-صفرم دیگر آفیس را تحت تأثیر قرار می‌دهد ولی هنوز وصله نشده است. شرکت مایکروسافت برای این منظور راه‌حل‌هایی را ارائه داده تا تأثیرات بهره‌برداری از این آسیب‌پذیری کاهش یابد. این آسیب‌پذیری در مقیاس محدود و در حملات هدف‌مند مورد بهره‌برداری قرار گرفته است.

اخبار فنی

مایکروسافت به‌روزرسانی امنیتی برای ماه آوریل را منتشر کرد

در به‌روزرسانی‌های امنیتی مایکروسافت برای ماه آوریل، تقریباً 40 آسیب‌پذیری حیاتی، مهم و متوسط وصله شده است. 3 مورد از این اشکالات، آسیب‌پذیری‌های روز-صفرم هستند که در حال حاضر در حملات فعال مورد بهره‌برداری قرار می‌گیرند.

به‌گزارش مایکروسافت این به‌روزرسانی‌ها آسیب‌پذیری در مرورگر اج، اینترنت اکسپلور، ویندوز، آفیس، ویژوال استادیو برای مک، چارچوب .NET، سیلورلایت و مؤلفه‌های ادوبی فلش پلیر را وصله کرده است.

یکی از آسیب‌پذیری‌های روز-صفرم که این ماه توسط مایکروسافت وصله شده، دارای شناسه‌ی CVE-2017-0199 بوده و آفیس و وردپد را تحت تأثیر قرار داده و با بهره‌برداری از آن می‌توان به اجرای کد از راه دور پرداخت. این آسیب‌پذیری در دنیای واقعی مورد بهره‌برداری قرار گرفته و برای توزیع بدافزارهایی مانند Dridex، WingBird، Latentbot و Godzilla مورد بهره‌برداری قرار می‌گیرد.

یکی دیگر از آسیب‌پذیری‌های روز-صفرم که در حال حاضر مورد بهره‌برداری قرار می‌گیرد دارای شناسه‌ی CVE-2017-0210 بوده و یک اشکال ارتقاء امتیاز است که اینترنت اکسپلورر را تحت تأثیر قرار می‌دهد. مایکروسافت می‌گوید این آسیب‌پذیری به‌خاطر نبود سیاست‌های کافی بین دامنه‌ها وجود دارد و می‌تواند با تحریک کاربر او را به صفحه‌ی وب مخرب و جعلی هدایت کند. هرچند مایکروسافت اطلاعاتی در مورد حملاتی که در حال حاضر رخ می‌دهد را به اشتراک نگذاشته است.

آسیب‌پذیری روز-صفرم دیگر در آفیس وجود داشته و مایکروسافت می‌گوید در حملات بسیار محدود و هدفمند مورد بهره‌برداری قرار گرفته است. این آسیب‌پذیری در به‌روزرسانی امنیتی این ماه وصله نشده است. با این‌حال مایکروسافت راه‌حل‌هایی را برای پیشگیری و کاهش خطرات این آسیب‌پذیری ارائه داده است. این آسیب‌پذیری در مؤلفه‌ی EPS آفیس وجود دارد و راه‌حلی که مایکروسافت ارائه داده این مؤلفه را به‌طور پیش‌فرض غیرفعال می‌کند.

در آسیب‌پذیری‌های حیاتی دیگری که مایکروسافت این هفته وصله کرده 13 مورد دیگر نیز وجود دارد که مرورگر اینترنت اکسپلورر، اج، چارچوب .NET، آفیس و هایپر وی را تحت تأثیر قرار داده است. مایکروسافت از ارائه‌ی بولتن‌های امنیتی به سمت پایگاه داده‌ی راهنمای به‌روزرسانی‌های امنیتی منتقل شده است. این ماه این انتقال تکمیل شده و هیچ بولتن امنیتی منتشر نشده است. در حالی‌که برخی کاربران از این تغییر استقبال کرده‌اند ولی برخی دیگر معتقدند با بولتن‌های امنیتی بیشتر ارتباط برقرار می‌کردند. همچنین شایان ذکر است، به‌روزرسانی این ماه، آخرین به‌روزرسانی برای ویندوز ویستا بوده است و از این به بعد برای این ویندوز به‌روزرسانی امنیتی منتشر نخواهد شد.

در کنار به‌روزرسانی‌های امنیتی مایکروسافت، شرکت ادوبی نیز روز سه‌شنبه به‌روزرسانی‌های مختلفی را برای محصولات خود منتشر کرده که در آن نزدیک به 60 آسیب‌پذیری در محصولات مختلف این شرکت وصله شده است. در ادوبی آکروبات و ریدر، 47 آسیب‌پذیری برطرف شده که بهره‌برداری موفق از آن‌ها منجر به اجرای کد دلخواه توسط مهاجم می‌شود. ادوبی می‌گوید شواهدی مبنی بر بهره‌برداری از این آسیب‌پذیری‌ها در دنیای واقعی مشاهده نکرده است.

اخبار فنی

آسیب‌پذیری روز-صفرم مایکروسافت ورد که در حال حاضر مورد بهره‌برداری قرار می‌گیرد

اینک در سال 2017 میلادی به سر می‌بریم و باز کردن یک پرونده‌ی مایکروسافت ورد می‌تواند سامانه‌ی شما را آلوده کند. محققان امنیتی هشدار دادند حمله‌ی جدیدی در حال حاضر انجام می‌شود که به‌طور کاملاً مخفیانه بدافزاری را با بهره‌برداری از یک آسیب‌پذیری روز-صفرم در نرم‌افزار مایکروسافت ورد، بر روی سامانه‌ای که کاملاً وصله شده است، نصب می‌کند. محققان می‌گویند این آسیب‌پذیری در مایکروسافت ورد بسیار جدی است و تاکنون وصله نشده است.

این آسیب‌پذیری روز-صفرم در مایکروسافت آفیس، توسط محققانی از شرکت‌های مک‌آفی و فایرآی کشف شده است. این حمله با ارسال یک رایانامه شروع می‌شود که در آن یک شیء مخرب OLE2link ضمیمه شده است. زمانی که این شیء مخرب باز می‌شود، کد بهره‌برداری اجرا شده و به کارگزار راه دور که در کنترل مهاجم است متصل می‌شود و از آن‌جا یک پرونده‌ی مخرب HTML را بارگیری می‌کند.

این پرونده‌ی HTML در ادامه به‌طور خودکار اجرا شده و بار داده‌های بیشتری را از بدافزارهای شناخته‌شده، بارگیری می‌کند تا سامانه‌ی هدف را از کار انداخته و در ادامه نیز پرونده‌ی ورد مخرب را می‌بندد. به گفته‌ی محققان امنیتی، این آسیب‌پذیری روز-صفرم بسیار جدی بوده و می‌تواند تمامی راه‌حل‌های دفاعی ارائه‌شده توسط مایکروسافت را دور بزند. همچنین این آسیب‌پذیری برای بهره‌برداری، برخلاف سایر آسیب‌پذیری‌ها نیاز ندارد تا کاربر ماکروها را فعال کند.

با این قابلیت‌هایی که گفته شد، حملات جدید بر روی تمامی سامانه عامل‌های ویندوز حتی ویندوز 10 کار می‌کند در حالی‌که به نظر می‌رسد ویندوز 10 یکی از امن‌ترین سامانه عامل‌های شرکت مایکروسافت است. ریشه‌ی این آسیب‌پذیری مربوط به یکی از ویژگی‌های مهم در مایکروسافت آفیس با نام OLE است.

محققان امنیتی می‌گویند مایکروسافت از این آسیب‌پذیری روز-صفرم باخبر است و پس از اینکه این اشکال وصله نشد و در حملات فعال در دنیای واقعی مورد بهره‌برداری قرار گرفت، محققان به‌طور مسئولانه این آسیب‌پذیری را افشاء کردند. ابتدا مک‌آفی این آسیب‌پذیری را به‌طور عمومی افشاء کرد و روز بعد نیز فایرآی جزئیات آن را منتشر نمود.

به‌روزرسانی امنیتی که در ادامه قرار است شرکت مایکروسافت داشته باشد، سه‌شنبه‌ی همین هفته منتشر خواهد شد و بسیار بعید به‌نظر می‌رسد این شرکت برای وصله‌ی این آسیب‌پذیری، به‌روزرسانی را زودتر از موعد منتشر کند.

اخبار فنی

هزاران مسیریاب آسیب‌پذیر برای حمله به وب‌گاه‌های وردپرس مورد استفاده قرار گرفتند

شرکت امنیتی Wordfence روز سه‌شنبه گزارش داد که ده‌ها هزار از مسیریاب‌های خانگی آسیب‌پذیر، مورد نفوذ قرار گرفته و برای حمله به وب‌گاه‌های وردپرس استفاده شده‌اند. این شرکت امنیتی ماه گذشته هشدار داد تعداد حملات علیه وب‌گاه مشتریان الجزایری نسبت به بازه‌ی مشابه گذشته افزایش یافته است. بررسی‌های دقیق‌تر 10 هزار آدرس IP حمله‌کننده را نشان داد که متعلق به یک شرکت مخابراتی در الجزایر بودند.

محققان امنیتی متوجه شدند مهاجمان از آسیب‌پذیری‌های موجود بر روی مسیریاب‌های این شرکت مخابراتی بهره‌برداری کرده و به آن‌ها نفوذ کرده‌اند. در ادامه از این دستگاه‌های آسیب‌پذیر برای اجرای حمله‌ی جستجوی فراگیر و سایر حملات بر روی وب‌گاه‌های وردپرس استفاده شده است.

محققان مسیریاب‌های آسیب‌پذیر را از 27 ارائه‌دهنده‌ی سرویس اینترنت (ISP) دیگر در سراسر جهان شناسایی کرده‌اند که در پاکستان، هند، فیلیپین، ترکیه، مصر، مراکش، مالزی، برزیل، اندونزی، صربستان، عربستان سعودی، روسیه، رومانی، سریلانکا، کرواسی و ایتالیا واقع شده‌اند. این مسیریاب‌ها بر روی درگاه باز 7547 به گوش هستند. این درگاه برای مدیریت مسیریاب‌های مشتریان توسط شرکت‌ها مورد استفاده قرار گرفته و از کارگزار وب AllegroSoft RomPager که دارای آسیب‌پذیری است، استفاده می‌کنند.

نسخه‌های قبلی 4.34 از کارگزار وب RomPager دارای آسیب‌پذیری حیاتی با شناسه‌ی CVE-2014-9222 هستند و بهره‌برداری از آن موجب سرقت مسیریاب‌های خانگی متعلق به شرکت‌های تولیدکننده‌ی مختلف می‌شود. افشای این آسیب‌پذیری به سال 2014 میلادی بر می‌گردد و محققان امنیتی هشدار دادند که نزدیک به 12 میلیون دستگاه آسیب‌پذیر در سراسر جهان وجود دارد.

ماه گذشته این شرکت امنیتی نزدیک به 90 هزار آدرس IP منحصربفرد را مشاهده کرده که به نظر می‌رسد متعلق به مسیریاب‌های خانگی آسیب‌پذیر هستند. محققان می‌گویند بیشتر این آدرس‌های IP در عرض 48 ساعت کمتر از هزار حمله را تولید کرده‌اند. این شرکت امنیتی ابزاری را به‌طور برخط منتشر کرده که کاربران با استفاده از آن می‌توانند باز بودن درگاه 7547 بر روی مسیریاب خانگی خود را بررسی کنند.

اخبار فنی

به‌روزرسانی BIND برای وصله‌ی 3 آسیب‌پذیری منع سرویس منتشر شد

کنسرسیوم سامانه‌های اینترنتی این هفته اعلام کرد به‌روزرسانی‌هایی برای نرم‌افزار DNS با نام BIND ارائه شده که 3 آسیب‌پذیری منع سرویس را برطرف می‌کند. این آسیب‌پذیری‌ها از راه دور قابل بهره‌برداری هستند. در 3 نسخه‌ی 9.10.4-P8، 9.9.9-P8 و 9.11.0-P5 این آسیب‌پذیری‌ها وصله شده است.

یکی از مهم‌ترین آسیب‌پذیری‌ها دارای شناسه‌ی CVE-2017-3137 است. این آسیب‌پذیری به مهاجم اجازه‌ی ایجاد شرایط منع سرویس را می‌دهد و عمدتاً تحلیل‌های DNS بازگشتی تحت تأثیر قرار می‌گیرند. کارگزارهای معتبر نیز اگر بخواهد پرس‌وجوهای بازگشتی انجام دهند، دارای آسیب‌پذیری هستند.

یکی دیگر از آسیب‌پذیری‌ها که در این به‌روزرسانی‌ها وصله شده، دارای شناسه‌ی CVE-2017-3136 است. درجه‌ی اهمیت این آسیب‌پذیری متوسط بوده و کارگزارهایی که برای استفاده DNS64 با گزینه‌ی

break-dnssec yes;

پیکربندی شده‌اند، تحت تأثیر قرار می‌دهد.

در سومین آسیب‌پذیری با شناسه‌ی CVE-2017-3138 می‌توان به فرآیند کارگزار نام BIND با ارسال دستور خالی خاتمه داد. با این‌حال تنها توسط مهاجمانی از راه دور قابل بهره‌برداری است که اجازه‌ی دسترسی به کانال‌های کنترلی را دارند.

گزارش‌ها حاکی از آن است که شواهدی مبنی بر بهره‌برداری از این آسیب‌پذیری‌ها در دنیای واقعی وجود ندارد. اوایل این ماه یک محقق امنیتی روشی جدید برای تشدید حملات منع سرویس بر روی نرم‌افزار BIND کشف کرد. این کارشناس امنیتی کشف کرد با استفاده از پاسخ پرس‌وجوهای DNAME ریشه، می‌توان حملات منع سرویس بر روی کارگزارهای DNS را تشدید کرد.

این مسئله به کنسرسیوم سامانه‌ی اینترنت گزارش شده اما این سازمان تشخیص داده که این حملات به دلیل آسیب‌پذیری در زمان طراحی پروتکل قابل انجام است و یک آسیب‌پذیری در خود نرم‌افزار BIND نیست. این محقق امنیتی اعلام کرد کارگزار DNS مایکروسافت در برابر چنین حملاتی آسیب‌پذیر نیست.

فصل پنجم

اخبار تحـــلیلی

اخبار تحلیلی

بدافزاری که برای جلوگیری از تشخیص، داده‌های ناخواسته تولید می‌کند

یک بدافزار جدید که در حملاتی کشورهای کره‌ی جنوبی و ژاپن را هدف قرار داده، برای جلوگیری از تشخیص به تولید داده‌های ناخواسته اقدام می‌کند. محققان آزمایشگاه کسپرسکی اعلام کردند هرچند این روش برای جلوگیری از تشخیص جدید نیست ولی عملیات این گروه قابل توجه است.

این شرکت امنیتی زمانی با این بدافزار مواجه شد که در حال بررسی حملات انجام‌شده توسط روت‌کیت XXMM بود. نام این بدافزار srvhost.exe بود و اندازه‌ای برابر با 100 مگابایت داشت و تلاش می‌کرد از بروز سوءظن جلوگیری کند.

بررسی‌های کسپرسکی نشان داد که این بدافزار یک تروجان بارگذاری‌کننده است که سعی دارد دربِ پشتی wali را فعال کند. ماژول دربِ پشتی توسط این بارگذاری‌کننده در پردازه‌ی iexplore.exe تزریق می‌شود. در نمونه‌های بدافزار که مشاهده شده، اندازه‌ی آن باتوجه به نوع بسته‌بندی از چند کیلوبایت تا چند مگابایت متغیر است. همچنین مشاهده شده مهاجمان سایبری بدافزار را در داخل پرونده‌های ISO و یا فیلم مخفی می‌کنند و این باعث می‌شود اندازه‌ی پرونده‌ی مخرب به چند گیگابایت هم برسد.

نکته‌ی جالب توجه در دربِ پشتی Wali این است که در قالب یک پرونده‌ی 100 مگابایتی بر روی سامانه‌ی قربانی قرار نمی‌گیرد. بارگذاری‌کننده‌ی اولیه اندازه‌ای برابر با 1 مگابایت دارد ولی مؤلفه‌های نصب‌کننده در ادامه می‌توانند به پرونده‌ی اجرایی بدافزار، حجمی برابر با ده‌ها مگابایت تا گیگابایت را اضافه کنند.

به‌خاطر اینکه داده‌های ناخواسته به‌طور پویا توسط نصب‌کننده تولید می‌شود، اندازه‌ی پرونده‌ی بدافزار می‌تواند متفاوت باشد. کسپرسکی در حملات واقعی نمونه‌هایی از بدافزار با اندازه‌ی 50 و 100 مگابایت را مشاهده کرده است. محققان امنیتی می‌گویند در حملاتی، اندازه‌ای برابر با 200 مگابایت را نیز شاهد بوده‌اند.

محققان امنیتی معتقدند این دربِ پشتی یک تهدید قابل توجه است چرا که در حملات هدفمند مورد استفاده قرار گرفته است. کسپرسکی در توضیحات خود می‌گوید: «هرچند در نگاه اول، این روش برای جلوگیری از تشخیص ناکارآمد به نظر برسد ولی در بررسی‌هایی که با ابزار YARA برای پویش دیسک انجام شده، ترافیک این بدافزار تشخیص داده نشده است.»

محققان کسپرسکی افزودند: «یکی از دلایل این مسئله این است که در پویش دیسک با ابزار YARA یکی از نکات مهم برای افزایش کارایی این است که اندازه‌ی پرونده‌هایی که پویش می‌شوند، کم در نظر گرفته شود. پرونده‌های بزرگی مانند نمونه‌ی بدافزار XXMM از دید این ابزار و قوانین آن مخفی خواهند ماند. بنابراین محققان امنیتی باید در زمان تنظیم قوانین برای ابزارهای امنیتی، به این موضوع نیز توجه داشته باشند.»

اخبار تحلیلی

بدافزار BrickerBot به ثابت‌افزار دستگاه‌های اینترنت اشیاء آسیب می‌رساند

محققان امنیتی گروه جدیدی از حملات سایبری را شناسایی کرده‌اند که دستگاه‌های اینترنت اشیاء را هدف حمله‌ی خود قرار داده‌اند و به‌جای تبدیل این دستگاه‌ها به بات‌نت به منابع این دستگاه آسیب می‌رسانند.

این حملات منع سرویس دائمی (PDoS) نام‌گذاری شده و بسیار مخرب هستند و پس از وقوع آن ضروری است تا دستگاه تعویض شده و یا سخت‌افزار آن مجدد نصب شود. محققان امنیتی توضیح دادند پس از بهره‌برداری از آسیب‌پذیری‌های این دستگاه‌ها، مهاجمان می‌توانند ثابت‌افزار و برنامه‌های سامانه‌ای را از کار بیندازند.

یکی از بدافزارهایی که در این نوع از حملات مورد استفاده قرار می‌گیرد، BrickerBot است که محققان امنیتی اخیراً دو نسخه‌ی مختلف از آن را مشاهده کرده‌اند. یکی از این نسخه‌ها عمر کوتاهی داشته و پس از مدتی غیرفعال باقی می‌ماند ولی نسخه‌ی دیگر همچنان به کار خود ادامه می‌دهد. با این‌حال هر دو نسخه هدف یکسانی دارند: آلوده کردن دستگاه اینترنت اشیاء و آسیب رساندن به منابع ذخیره‌شده بر روی دستگاه.

هر دوی این نسخه از بدافزار، در یک تاریخ مشخص حملات منع سرویس دائمی را شروع کرده و محققان آن‌ها را با فاصله‌ی یک ساعت از هم کشف کرده‌اند. نسخه‌ی اول از بدافزار که دارای عمر کوتاهی است، حملات شدیدتری انجام می‌دهد در حالی‌که نسخه‌ی دیگر شدت کمتری داشته ولی حملات آن دقیق‌تر است و برای مخفی شدن از شبکه‌ی گمنامی Tor بهره می‌برد.

برای آلوده کردن دستگاه اینترنت اشیاء، بدافزار BrickerBot از حمله‌ی جستجوی فراگیر بر روی پروتکل telnet استفاده می‌کند. این روش قبلاً نیز در حملات بدافزار Mirai مورد استفاده قرار گرفته بود تا دستگاه‌ها را آلوده کرده و از آن‌ها برای حملات منع سرویس توزیع‌شده استفاده کند.

پس از دسترسی موفق به دستگاه مورد نظر، بدافزار برخی دستورات لینوکسی را برای خراب کردن منابع ذخیره‌سازی دستگاه اجرا می‌کند. در ادامه نیز تلاش دارد اتصال دستگاه به اینترنت را قطع کرده و تمامی پرونده‌های موجود بر روی دستگاه آلوده را حذف کند.

این حمله بیشتر دستگاه‌های اینترنت اشیاء مبتنی بر سامانه‌های لینوکس را که درگاه telnet در آن‌ها باز بوده و از طریق اینترنت قابل دسترسی است، هدف قرار می‌دهد. دستگاه‌هایی که هدف حمله‌ی بات‌نت Mirai قرار گرفته بودند، در برابر حمله‌ی بات‌نت جدید نیز آسیب‌پذیر هستند.

حملات منع سرویس دائمی، از روی تعداد محدودی از آدرس‌های IP انجام شده و بر روی تمامی عامل‌ها، درگاه 22 باز بوده و از یک نسخه‌ی بسیار قدیمی کارگزار Dropbear SSH استفاده می‌کردند. محققان امنیتی نوع دوم از حملات منع سرویس دائمی را نیز شناسایی کردند

کـه در آن آدرس‌هـای IP پشـت یـک شـبکه‌ی Tor مخفـی می‌شـود. ایـن حمـلات همچنـان ادامـه داشـته و بـر روی سرویـس telnet حمـلات جسـتجوی فراگیـر بـا نـام کاربـری و گذرواژه‌هـای root/root و root/vizxv انجـام می‌دهنـد. در ادامـه نیـز بـرای آسـیب بـه منابـع ذخیره‌سـازی دسـتگاه، دسـتورات لینوکسـی دیگـری اجـرا می‌شـود.

محققـان امنیتـی می‌گوینـد در ایـن حمـلات از ابـزار busybox اسـتفاده نشـده ولـی مهاجـمان از ابزارهـای dd و cat کـه بـر روی دسـتگاه‌های آلـوده وجـود دارد، اسـتفاده می‌کننـد. در نهایـت در ایـن حمـلات تـلاش می‌شـود تـا دروازه‌ی پیش‌فـرض بـر روی دسـتگاه حـذف شـده و مُهرزمانـی TCP غیرفعـال شـود. بـا کمـک دسـتورات اضافـی دیگـر، مهاجـمان تـلاش می‌کننـد تمامـی قوانیـن iptable و NAT را حـذف کـرده و قوانیـن جدیـدی بـرای رهـا کـردن تمـام بسـته‌های خروجـی اعـمال کننـد.

اخبار تحلیلی

باتنت Amnesia و حمله به دستگاه‌های آسیب‌پذیر اینترنت اشیاء

یک باتنت لینوکسی جدید با نام Amnesia دستگاه‌های ضبط ویدئوی دیجیتال (DVR) را هدف قرار داده است. این باتنت از یک آسیب‌پذیری اجرای کد از راه دور بر روی این دستگاه‌ها بهره‌برداری می‌کند. این آسیب‌پذیری تقریباً یک سال قبل کشف و گزارش شده ولی هنوز بر روی تعداد کثیری از دستگاه‌ها، این آسیب‌پذیری وصله نشده است.

تصور می‌شود این باتنت نسخه‌ای از باتنت سونامی است که توسط محققان شرکت پالوآلتو مورد بررسی و تحلیل قرار گرفته بود. این باتنت سامانه‌های تعبیه‌شده بویژه دستگاه‌های DVR ساخت کشور چین را هدف قرار داده است. این محصولات در بیش از 70 مدل در سراسر جهان به فروش رسیده‌اند. این آسیب‌پذیری سال قبل توسط یک محقق امنیتی کشف شد و پس از اینکه شرکت سازنده به گزارش او توجهی نکرد، جزئیات این آسیب‌پذیری را به‌طور عمومی افشاء کرد.

به احتمال زیاد این آسیب‌پذیری وصله نشده باقی مانده و پویش‌هایی که توسط شرکت پالوآلتو انجام شده نشان می‌دهد که در کشورهای آمریکا، تایوان، هندوستان، رژیم صهیونیستی، ترکیه و مالزی بیش از 227 هزار دستگاه آسیب‌پذیر وجود دارد. در تحقیق جداگانه، گروه دیگری از محققان امنیتی نشان دادند که در این حمله بیش از 700 هزار آدرس IP منحصربفرد مشارکت داشتند.

در چند ماه گذشته شاهد فعالیت‌های زیادی از سمت باتنت‌های اینترنت اشیاء مانند Mirai و Remaiten هستیم. در مورد این باتنت جدید، چیزی که جالب توجه است این نکته است که بدافزار اجرا بر روی ماشین مجازی را بررسی کرده و تلاش دارد اجرا شدن بر روی چنین محیط‌های تحلیلی و آزمایشی را دور بزند. کارشناسان امنیتی می‌گویند این اولین بدافزار لینوکسی است که سعی دارد محیط جعبه شنی را دور بزند.

در مورد بدافزارهای ویندوز و اندروید معمولاً شاهد هستیم که تلاش دارند از اجرا بر روی ماشین‌های مجازی اجتناب کنند ولی در مورد بدافزارهای لینوکسی تاکنون چنین موردی مشاهده نشده بود. محققان می‌گویند اگر بدافزار اجرا بر روی ماشین مجازی را تشخیص دهد، با حذف کردن پرونده‌های سامانه، تلاش می‌کند تا کل ماشین مجازی را حذف کند.

هرچند باتنت Amnesia برای اجرای حملات وسیع و گسترده به کار گرفته نشده است ولی محققان معتقدند این باتنت پتانسیل تبدیل شدن به باتنت بزرگ و قوی را دارد که در حملات آینده علیه دستگاه‌های اینترنت اشیاء خطرساز باشد.

اخبار تحلیلی

بهره‌برداری از آسیب‌پذیری روز-صفرم آفیس برای توزیع تروجان بانکی Dridex

آسیب‌پذیری روز-صفرم که اخیراً در مایکروسافت آفیس کشف شده، توسط تروجان بانکی Dridex مورد بهره‌برداری قرار می‌گیرد تا رایانه‌های قربانیان را آلوده کند. جزئیات این آسیب‌پذیری توسط مک‌آفی و فایرآی تشریح شده و بهره‌برداری موفق از آن به مهاجم اجازه اجرای دستورات بر روی رایانه‌ی آلوده را می‌دهد.

با استفاده از قابلیت OLE در آفیس، مهاجم می‌تواند یک سند RTF ایجاد کند که به یک پرونده‌ی HTML بر روی کارگزار راه دور پیوند دارد. این پرونده‌ی HTML در ادامه قابلیت اجرای یک اسکریپت مخرب ویژوال بیسیک را دارد. محققان پروف‌پوینت می‌گویند این آسیب‌پذیری در اسناد مخربی که در رایانامه‌ها برای هزاران قربانی ارسال شده، مورد بهره‌برداری قرار می‌گیرد. این رایانامه‌های مخرب در ادامه منجر به نصب بدافزار Dridex بر روی ماشین قربانی می‌شود.

در این پویش تمامی پیام‌ها از طرف آدرسی به شکل <[device]@[recipient's domain] ارسال شده که در بخش [device] عباراتی مانند copier، documents، no-reply، noreply و یا scanner می‌تواند قرار بگیرد.

موضوع رایانامه در تمامی موارد Scan Data است در حالی‌که نام سند مخرب مایکروسافت ورد Scan_xxxx. doc یا Scan_xxxx.pdf است.

وقتی این سند مخرب باز شد، بهره‌برداری انجام شده و پس از اجرای یک سری دستورات، تروجان Dridex با شناسه‌ی 7500 بر روی رایانه‌ی قربانی نصب می‌شود. محققان امنیتی اشاره کردند برای بهره‌برداری از این آسیب‌پذیری هیچ نیازی به تعامل کاربر وجود ندارد. محققان امنیتی می‌گویند در چند وقت اخیر شاهد بوده‌ایم که مهاجم از طریق هرزنامه و ماکروهای مخرب سعی در نصب بدافزار داشتند و برای فریب کاربر از روش‌های مهندسی اجتماعی بهره می‌بردند ولی در این حمله می‌بینیم که هیچ یک از این موارد رخ نداده است. به‌عبارت دیگر مهاجمان می‌توانند به راحتی روش‌های مورد استفاده‌ی خود را تغییر داده و تأثیر عملیات خود را افزایش دهند.

اخبار تحلیلی

نسخه‌ی جدید بدافزار Mirai دارای قابلیت استخراج بیت‌کوین است

محققان امنیتی هشدار دادند که نسخه‌ی جدیدی از بدافزار Mirai مشاهده شده که دستگاه‌های اینترنت اشیاء را برای استخراج ارز مجازی بیت‌کوین هدف قرار داده است. بدافزار Miari اولین بار در سپتامبر سال گذشته مورد بررسی قرار گرفت و تلاش دارد دستگاه‌های آسیب‌پذیر اینترنت اشیاء را شناسایی کرده و آن‌ها را به بات تبدیل کند. این بات‌ها در ادامه برای انجام حمله‌ی منع سرویس توزیع‌شده مورد استفاده قرار می‌گیرند.

از زمانی‌که کد منبع این بدافزار به‌طور عمومی منتشر شد، نسخه‌های مختلفی از آن را شاهد بودیم. اوایل سال جاری نیز نسخه‌ی ویندوزی بدافزار ظاهر شد که برای گسترش نسخه‌ی لینوکسی بدافزار مورد استفاده قرار می‌گرفت. در نسخه‌ای که اخیراً مشاهده شده، علاوه بر قابلیت حمله‌ی منع سرویس، قابلیت استخراج بیت‌کوین نیز اضافه شده است.

این نسخه از Mirai که قابلیت استخراج بیت‌کوین را دارد، در یک پویش کوتاه‌مدت در اواخر ماه مارس مشاهده شده است که ماشین‌های لینوکسی که BusyBox را اجرا می‌کنند هدف قرار داده است. در این حملات تمرکز اصلی بر روی کارگزارهای DVR و بهره‌برداری از پروتکل telnet قرار دارد. بدافزار Miari برای حمله به دستگاه‌های اینترنت اشیاء، از پروتکل telnet با انجام حمله‌ی جستجوی فراگیر استفاده می‌کند.

علاوه بر قابلیت‌هایی که تاکنون از بدافزار Mirai شاهد بوده‌ایم، نسخه‌ی جدید بدافزار می‌توان ماشین قربانی را به برده‌ای برای استخراج بیت‌کوین تبدیل کند. به‌دلیل اینکه دستگاه‌های اینترنت اشیاء دارای توان پردازشی پایین هستند، به خودی خود نمی‌توانند به استخراج بیت‌کوین بپردازند.

محققان امنیتی در توضیحات خود گفتند: «هرچند دستگاه‌های اینترنت اشیاء به تنهایی نمی‌توانند به درستی برای استخراج بیت‌کوین مورد استفاده قرار گیرند ولی این بات‌های آلوده در کنار هم می‌توانند مقدار ارزشمندی بیت‌کوین استخراج کنند. احتمالاً زمانی‌که این بات‌ها بیکار هستند و دستوری برای اجرا دریافت نکرده‌اند، مشغول استخراج بیت‌کوین می‌شوند.»

بدافزار Mirai آخرین بدافزاری است که قابلیت استخراج ارز مجازی را بدست آورده است. آخرین موردی که قبلاً این قابلیت را داشت، کیت بهره‌برداری Sundown بود که چند ماه قبل به استخراج ارز مجازی Monero می‌پرداخت. سال گذشته محققان امنیتی یک تروجان لینوکسی را کشف کردند که به زبان Go نوشته شده بود و بر روی استخراج Monero تمرکز داشت.

اخبار تحلیلی

سازمان OWASP برای سال 2017 میلادی آسیب‌پذیری‌های جدیدی منتشر کرد

پروژه‌ی باز برنامه‌های کاربردی تحت وب (OWASP) روز دوشنبه سری جدیدی از 10 آسیب‌پذیری برتر در برنامه‌های وب در سال 2017 را اطلاع‌رسانی کرد که در آن 2 دسته آسیب‌پذیری جدید معرفی شده است. این دو دسته‌ی جدید عبارتند از «تشخیص و پیشگیری ناکافی از حملات» و «واسط‌های برنامه‌نویسی محافظت‌نشده».

پروژه‌ی OWASP قصد دارد در فهرست 10 آسیب‌پذیری برتر خود که آخرین بار در سال 2013 میلادی به‌روزرسانی شده، آسیب‌پذیری «تغییر مسیر نامعتبر» را حذف کرده و آسیب‌پذیری «واسط‌های برنامه‌نویسی حفاظت‌نشده» را اضافه کند.

آسیب‌پذیری «تشخیص و پیشگیری ناکافی از حملات» نیز در این فهرست در ردیف هفتم قرار گرفته است. برای جا دادن این آسیب‌پذیری، OWASP دو آسیب‌پذیری موجود در ردیف‌های 4 و 7 را با یکدیگر ادغام کرده است. این آسیب‌پذیری‌ها «ارجاع مستقیم به اشیاء به‌طور ناامن» و «عدم وجود کنترل دسترسی در سطح برنامه‌های کاربردی» هستند. این سازمان نام این آسیب‌پذیری ادغامی را «کنترل دسترسی ناقص» قرار داده است.

تعریفی که OWASP برای آسیب‌پذیری تشخیص و پیشگیری ناکافی از حملات ارائه داده به شرح زیر است: «اکثر برنامه‌های کاربردی و واسط‌های برنامه‌نویسی فاقد روشی برای تشخیص و پیشگیری از حملات دستی و خودکار هستند. حفاظت در برابر حملات، چیزی فراتر از اعتبارسنجی ورودی‌ها بوده و شامل تشخیص خودکار، ثبت رویدادها، پاسخ‌دهی و حتی مسدود کردن عملیات است. مالکان برنامه‌های کاربردی باید قادر باشند برای پیشگیری از حملات هرچه سریع‌تر وصله‌ها را اعمال کنند.»

در بحثی که در انجمن Reddit انجام شده بسیاری از کاربران اعلام کردند حفاظت ناکافی در برابر حملات نمی‌تواند به‌عنوان یک آسیب‌پذیری طبقه‌بندی شود. اگر کاربران زیادی با این تغییر موافق باشند، OWASP این تغییرات را اعمال خواهد کرد.

در دسته‌ی واسط‌های برنامه‌نویسی حفاظت‌نشده، OWASP می‌گوید: «برنامه‌های کاربردی مدرن معمولاً دارای کارخواه و واسط‌های برنامه‌نویسی غنی هستند که آن‌ها را به واسط‌های برنامه‌نویسی دیگر متصل می‌کند. این واسط‌ها معمولاً محافظت نمی‌شوند و تعداد زیادی آسیب‌پذیری در آن‌ها وجود دارد.»

نظرات برای طرح پیشنهادی OWASP برای فهرست 10 آسیب‌پذیری برتر تا تاریخ 30 ژوئن از طریق رایانامه‌ی OWASP-TopTen(at)lists.owasp.org قابل ارسال است. نسخه‌ی نهایی در ماه ژوئیه و یا اوت منتشر خواهد شد.

اخبار تحلیلی

غیرفعال شدن کیت بهره‌برداری Sundown و ظهور کیت جدید با نام ترور

بعد از گذشت یک سال از تغییر و تحول ناگهانی در حوزه‌ی کیت‌های بهره‌برداری که با ناپدید شدن کیت‌های Angler و Nuclear رخ داد، اینک شاهد تحولات دیگری هستیم. محققان امنیتی می‌گویند تقریباً یک ماه می‌شود که کیت بهره‌برداری Sundown به حالت غیرفعال درآمده و در پویش‌های جدید سایبری از کیت بهره‌برداری جدیدی با نام ترور استفاده می‌شود.

هرچند که کیت بهره‌برداری Sundown نیز خیلی در بازار دارای سهم بالایی نبود و بعد از ناپدید شدن کیت Neutrino بیشتر توسط مهاجمان سایبری مورد استفاده قرار می‌گرفت ولی تا پایان سال گذشته، هنوز نتوانسته بود در بین 3 کیت بهره‌برداری برتر قرار بگیرد.

توسعه‌دهندگان کیت بهره‌برداری Sundown بسیار فعال بودند و تلاش می‌کردند تمامی فناوری‌های جدید را در کیت خود بگنجانند. اخیراً شاهد بودیم که قابلیت نهان‌نگاری هم به این کیت اضافه شده بود تا بهره‌برداری‌ها در پرونده‌های تصویری به ظاهر بی‌خطر مخفی شود.

با این‌حال، محققان امنیتی یک ماه می‌شود که از غیرفعال شدن این کیت بهره‌برداری خبر می‌دهند به‌طوری که نسخه‌های مختلف این کیت نیز ناپدید شده است. همزمان با غیرفعال شدن این کیت، کیت بهره‌برداری دیگری با نام ترور ظاهر شده است. این کیت برای اولین بار در ماه ژانویه مشاهده شد و گفته می‌شود نسخه‌ای از کیت Sundown است چرا که مشابهت زیادی بین کدهای آن‌ها وجود دارد.

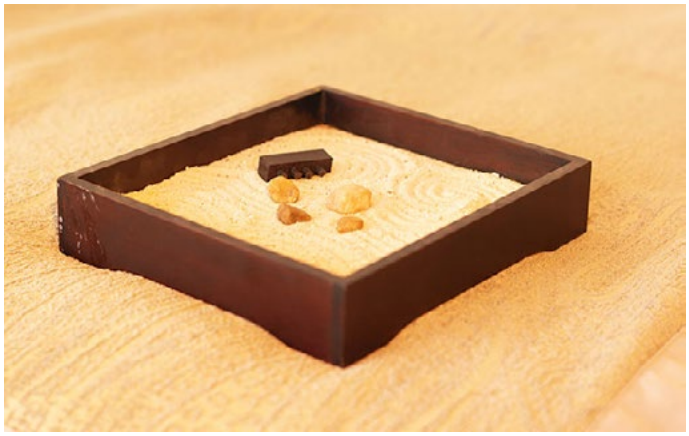
نویسنده‌ی این کیت بهره‌برداری که محققان امنیتی او را در انجمن‌های زیرزمینی مختلف با شناسه‌ی @666_ KingCobra پیدا کرده‌اند، این کیت را با نام‌های مختلف به فروش می‌رساند. ظاهراً این کیت با نام‌های دیگری مانند Neptune، Blaze و Eris نیز شناخته می‌شود.

مهم‌ترین نمونه از این کیت بهره‌برداری در پویش تبلیغ‌افزاری با نام Smoke Loader مورد استفاده قرار گرفته است. استفاده از شبکه‌های تبلیغاتی متنوع که ترافیکی با کیفیت پایین تولید می‌کنند از ویژگی‌های بارز این پویش بوده و از اینترنت اکسپلورر، فلش و سیلورلایت برای آلوده کردن سامانه‌ی قربانی بهره‌برداری می‌کند.

محققان امنیتی می‌گویند کیت بهره‌برداری Sundown به سرقت بهره‌برداری‌ها از سایر کیت‌ها معروف بود و از ویژگی‌های دیگر کیت‌ها استفاده می‌کرد. اگر این رویکرد توسط کیت‌های بهره‌برداری دیگر نیز مورد استفاده قرار می‌گرفت، با تهدید بسیار قوی‌تری مواجه بودیم ولی در حال حاضر چنین نیست.

اخبار تحلیلی

تروجان اندرویدی برای فرار از تشخیص از جعبه شنی استفاده می‌کند



محققان امنیتی از شرکت آواست اعلام کردند بدافزار Triada که سال قبل به‌عنوان یکی از پیشرفته‌ترین تهدیدات در حوزه‌ی تلفن‌های همراه شناسایی شد، قابلیت‌های جلوگیری از تشخیص خود را بهبود داده و با برخی از ویژگی‌های محیط جعبه شنی سازگار شده است. این بدافزار برای اولین بار، سال گذشته مورد بررسی قرار گرفت که از فرآیند Zygote برای قلاب کردن برنامه‌های موجود بر روی دستگاه استفاده می‌کرد. داشتن ویژگی ماژولار در این بدافزار برای هدایت و تغییر مسیر پیامک‌های مالی برای خرید محتوای بیشتر یا سرقت پول کاربر مورد استفاده قرار می‌گیرد.

بدافزار Triada به تازگی استفاده از جعبه شنی متن‌باز DroidPlugin را آغاز کرده است که بدون نصب یک برنامه می‌تواند آن را بارگیری و اجرا نماید. با کمک این جعبه شنی، بدافزار برنامه‌های مخرب اندروید را بارگذاری کرده و بدون نصب آن‌ها بر روی دستگاه، به اجرای آن‌ها می‌پردازد. با این اقدام، کشف بدافزار برای راه‌حل‌های ضدبدافزاری بسیار سخت می‌شود چرا که هیچ پرونده‌ی مخربی در قسمت برنامه‌های میزبان نصب نشده است.

این بدافزار با استفاده از روش‌های مهندسی اجتماعی و تحریک کاربر به بارگیری و نصب آن توزیع می‌شود. پس از نصب، بدافزار آیکون خود را از صفحه‌ی نمایش تلفن همراه مخفی کرده و در پس‌زمینه به سرقت اطلاعات می‌پردازد بدون اینکه به کاربر قربانی هشداری بدهد. هرچند نسخه‌های قبلی از این بدافزار از جعبه شنی DroidPlugin استفاده نمی‌کردند، ولی محققان از آبان ماه سال گذشته مشاهده کردند که بدافزار با روش‌های این جعبه شنی مطابقت پیدا کرده است. با آغاز استفاده از این جعبه شنی توسط بدافزار Triada نویسنده‌ی بدافزار یک آسیب‌پذیری خارج از محدوده‌ی حافظه را در این ابزار کشف و به توسعه‌دهنده‌ی آن گزارش داده است.

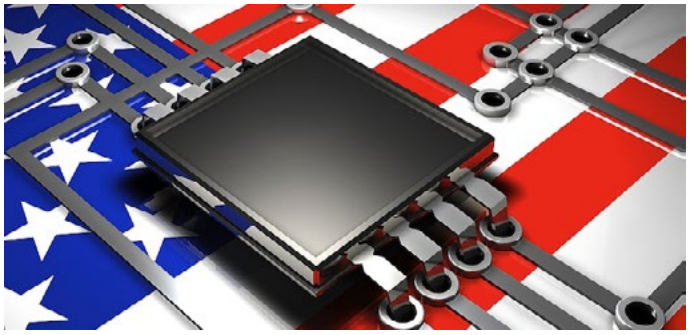
به گزارش محققان امنیتی، بدافزار خود را در قالب برنامه‌ی Wandoujia که یک فروشگاه معروف برنامه‌های اندروید در چین است، مخفی می‌کند. علاوه بر این مشاهده شده این بدافزار تمامی افزونه‌های خود را برای اجرا شدن در پوشه‌ی جعبه شنی DroidPlugin قرار داده است. محققان می‌گویند: «هریک از این افزونه‌ها عملیات مخرب مخصوص به خود را انجام می‌دهند. به‌عنوان مثال یکی از این افزونه‌ها با کارگزار دستور و کنترل ارتباط برقرار کرده و دستورات لازم برای اجرای افزونه‌ها را دریافت می‌کند. این دستورات دریافت‌شده باید توسط افزونه‌های دیگر انجام شوند.»

محققان همچنین اشاره کردند، نویسنده‌ی این بدافزار، افزونه‌های مخرب را در قالب یک برنامه با هم ادغام نکرده تا هریک از افزونه‌ها قابلیت بارگیری و اجرا توسط جعبه شنی DroidPlugin را داشته باشند. برنامه‌ی میزبان که نصب شده، دارای هیچ فعالیت مخربی نبوده و توسط

برنامه‌های ضدبدافزار شناسایی و مسدود نخواهد شد.
تاکنون تعداد بسیار محدودی از بدافزارها مشاهده شده‌اند که برای اهداف مخرب خود از روش‌های جعبه شنی استفاده می‌کنند ولی باید پس از این، شاهد افزایش استفاده از چنین روش‌هایی باشیم. باتوجه به این ویژگی که جعبه شنی بدون نصب یک برنامه می‌تواند آن را اجرا کند، این روش می‌تواند توسط بدافزارهای مختلف مورد استفاده قرار بگیرد.

اخبار تحلیلی

دارپا: ویژگی‌های امنیتی باید بر روی مدارهای سخت‌افزاری تعبیه شود



آژانس پروژه‌های تحقیقاتی پیشرفته‌ی وزارت دفاع آمریکا (دارپا) این هفته برنامه‌ای را اطلاع‌رسانی کرد که مدعی است در آن قرار است محافظت‌ها در برابر نفوذ به‌طور مستقیم بر روی سخت‌افزار پیاده‌سازی شوند.

این آژانس اشاره کرد که بسیاری از مدارهای مجتمع دارای آسیب‌پذیری هستند که از طریق نرم‌افزارها مورد بهره‌برداری قرار می‌گیرد. وصله‌های نرم‌افزاری نیز صرفاً راه‌حل‌های موقتی هستند. در بخشی از برنامه‌ی 39 ماهه با نام سامانه‌ی امنیتی در ثابت‌افزار و سخت‌افزار (SSITH) دارپا امیدوار است پیشنهادهای پژوهشی خوبی را برای توسعه‌ی تراشه‌های امن دریافت کند و جلوی بهره‌برداری نرم‌افزاری از آسیب‌پذیری‌های سخت‌افزار گرفته شود.

این پروژه بر روی 2 حوزه‌ی فنی بسیار مهم تمرکز دارد: توسعه‌ی معماری سخت‌افزاری امن و معرفی ابزاری برای تولیدکنندگان تا از این نوآوری‌های امنیتی استفاده کرده و با استفاده از معیارهایی، وضعیت امنیتی سامانه‌های جدید را شناسایی کنند.

در حال حاضر بسیاری از تولیدکنندگان مدارهای مجتمع مانند اینتل، ویژگی‌های محافظتی مختلفی را در تراشه‌های خود تعبیه کرده‌اند اما دارپا می‌خواهد ابزاری را توسعه دهد که در سطح گسترده‌ای مورد استفاده قرار بگیرد و امنیت تعبیه‌شده در سخت‌افزار به یک استاندارد در وزارت دفاع آمریکا و سایر شرکت‌های تجاری تبدیل شود.

دارپا اعلام کرده پیشنهادهای پژوهشی که ارائه می‌شود باید 7 مورد از آسیب‌پذیری‌های سخت‌افزاری که در فهرستی معرفی شده را برطرف کند. این آسیب‌پذیری‌ها شامل تزریق کد، مجوزها و امتیازات، خطاهای بافر، نشت اطلاعات، مدیریت منابع، خطاهای عددی و اشکالات رمزنگاری است. این آژانس اشاره کرده در 2800 مورد از حوادث امنیتی از این نوع آسیب‌پذیری‌ها بهره‌برداری شده و با برطرف کردن این اشکالات می‌توان تا 40 درصد از ضعف‌های امنیتی پیشگیری کرد.

Expert Bulletin News

اخبار فناوری اطلاعات و ارتباطات

هفته نامه | شماره صد و هشم | سال سوم | ۳۷ صفحه

خبرنامه هفتگی کارشناسی

مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج