شماره دهم - آبان ۱۳۹۶

خبرنامه "آپا" دانشگاه خوارزمی

در این شماره خواهید خواند:

آسیب پذیری در تمام پردازه‌های اینتل!

تقریبا تمام پردازنده های شرکت اینتل از زمان ایجاد معماری Skylake نسبت به حمله های مبتنی بر USB آسیب پذیر بوده اند. - صفحه ۲

- **باج افزار BadRabbit**

نسل جدیدی از باج افزار به نام "خرگوش بد" در روسیه، اوکراین و سایر بخش‌های شرقی اروپا در حال گسترش می‌باشد. به نظر می‌رسد که علارغم شباهت‌های موجود با باج افزار Petya اما از آن متفاوت می‌باشد. از این رو این باج افزار توانسته است باعث ویرانی در سیستم رسانه‌ای، حمل و نقل عمومی و یک فرودگاه در اکراین گردد. - صفحه ۵

باگ در DNS ویندوز

در سرویس DNS، ویندوز ۸، ویندوز ۱۰، ویندوز سرور ۲۰۱۲ و ویندوز سرور ۲۰۱۶ ، باگی ردیابی شده است. - صفحه ۹

هشدار Watchdog از آسیب پذیری-های امنیتی در ساعت‌های هوشمند کودکان

نگرانی‌های امنیتی در مورد اسباب بازی‌های مرتبط با کودکان، مسئله جدیدی نیست. عروسک‌های با قابلیت Wi-Fi مانند MyFriend Cayla و Barbie در معرض آسیب پذیری هکرها قرار گرفتند. - صفحه ۳

- **بازگشت دوباره باج افزار Matrix**

محقق امنیتی شرکت Malwarebytes به نام Jérôme Segura دریافته است که باج افزار ماتریکس با استفاده از کیت اکسپلویت RIG برروی سایت‌هایی که میزبان بدافزارهای تبلیغاتی هستند مجددا در حال گسترش می‌باشد. - صفحه ۶ و ۷

- **پچ آسیب پذیری‌های KRACK در اندروید WPA2**

گوگل پچ لازم برای رفع آسیب پذیری KRACK که در ماه گذشته منتشر شد را فراهم نمود. - صفحه ۱۰

معرفی سرویس امنیتی جدید گوگل برای دفع حملات سایبری

با تحقیقات امنیتی در حال انجام در روسیه پیرامون آسیب پذیری گسترده Equifax، گوگل در حال معرفی سرویس جدیدی است که امنیت سیستم احراز هویت دو مرحله ای را بهبود می‌بخشد. - صفحه ۴

هک آیفون ۷ توسط Pwn2Own

امنیت آیفون ۷ توسط یک گروه سه نفره از هکرها در رویداد موبایل Pwn2Own با استفاده از یک آسیب پذیری در wi-fi، یک باگ در سیستم خدمات و دو باگ در Safari به مخاطره افتاد. - صفحه ۸

- **MineCraft و سرقت اطلاعات کاربران!**

بازی Minecraft با میلیون بازی کننده فرصت جدیدی است که جنایتکاران سایبری به آن دست یافته‌اند. - صفحه ۱۱

آسیب پذیری در تمام پردازه‌های اینتل!

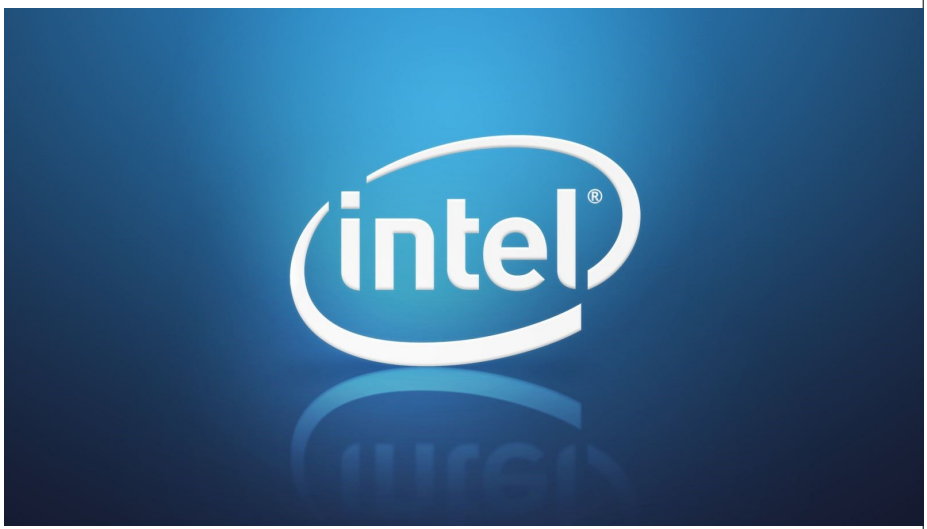
تقریبا تمام پردازنده های شرکت اینتل از زمان ایجاد معماری Skylake نسبت به حمله های مبتنی بر USB آسیب پذیر بوده اند.

موتور مدیریت اینتل توسط اکثر کاربران نادیده گرفته می شود، اما این زیر سیستم در سیستم های مبتنی بر اینتل نقش بسیار مهمی را ایفا می کند. از سال ۲۰۰۸، تقریبا هر پردازنده ای که توسط این شرکت منتشر شد، دارای IME است که برخی از آنها رایانه ای در دل رایانه شما هستند و قابلیت های بسیار خوبی دارند. در یک نمودار معماری کامپیوتر، IME بالاتر از CPU و قبل از سیستم عامل قرار دارد. هدف آن کنترل CPU، سخت افزارهای دیگر و انجام کارها به صورت remote با دسترسی administrator است.

صندوق بین المللی پول سالها ادعا میکردند که این "جعبه سیاه" تهدید امنیتی بزرگی است؛ زیرا می تواند سیستم شما را حتی زمانی که رایانه خاموش است کنترل کند. این ترس ها بعد از آنکه محققان امنیتی یک سوءاستفاده مبتنی بر USB را کشف کردند به واقعیت بدل گشت.

شرکت، فن آوری های مثبت تقریبا می تواند بر روی هر رایانه ای که IME را از طریق USB اجرا می کند، کد های بدون علامت ، اجرا کند. حمله با استفاده از پورت های اشکال زدایی JTAG ساخته شده به کامپیوتر کار می کند. بسیاری از دستگاه ها از جمله IME و USB به این پورت ها متصل می شوند، در واقع قرار است این مکانیزم بین آنها تقسیم شوند. محققان راهی را برای از بین بردن این موانع کشف کرده اند آنها کد خود را از یک فلش مموری اجرا می کنند.

محققان آسیب پذیری های قبلی را با موتور مدیریت اینتل شناسایی کرده اند، یکی از ویژگی های منحصر به فرد توجه به کاربرد آسان آن است. در حال حاضر این فقط یک اثبات مفهوم است که فقط Skylake (۲۰۱۵) و سیستم عامل های جدیدتر را تحت تاثیر قرار می دهد. بدون شک اینتل به زودی این پچ را تغییر خواهد داد، اما هنوز هم برای بسیاری از آنها این مسئله نگران کننده است. هیچ راهی برای غیرفعال کردن IME وجود ندارد زیرا این ویژگی بخشی از CPU فیزیکی است. بدون یک پچ، تنها راه محافظت در برابر این حمله تغییر سیستم عامل IME است.



گردآورنده: سمیه نیاخلیلی

هشدار Watchdog از آسیب پذیری‌های امنیتی در ساعت‌های هوشمند کودکان

نگرانی‌های امنیتی در مورد اسباب بازی‌های مرتبط با کودکان، مسئله جدیدی نیست. عروسک‌های با قابلیت Wi-Fi مانند MyFriend Cayla و Barbie در معرض آسیب پذیری هکرها قرار گرفتند، در حالی که اسباب بازی هوشمند Fisher-Price و HereO watches نیز دارای حفره‌های امنیتی خطرناکی بودند که از آن زمان تا کنون تولید نشده اند. در حال حاضر، یکی از ناظرین watchdog در مورد خطرات ساعت‌های هوشمند طراحی شده برای کودکان هشدار داده است.

شورای مصرف کننده نروژ (NCC) تعدادی از این ساعت‌ها را که مناسب کودکان می‌باشد را آزمایش کرده است، از جمله Gator و GPS. این دستگاه‌ها به والدین اجازه می‌دهند مکان فرزندان خود را (از طریق یک برنامه گوشی هوشمند) نظارت کنند، حتی می‌توانند تماس تلفنی را به مجموعه‌ای از اعداد محدود کنند. این دستگاه همچنین دارای یک دکمه SOS و قابلیت geofencing است که هشداری در صورت ترک کودک از محلی خاص ارسال می‌کند.

اما NCC و شرکت امنیتی Mnemonic دریافتند که امنیت ضعیف این دستگاه‌ها هکرها را قادر به ردیابی مصرف کنندگان، تغییر محل نگهداری کودک، گوش دادن به گفتگوها و به خطر انداختن کلید اضطراری می‌کند.

همچنین کشف کردند که برخی از ساعت‌ها اطلاعات ذخیره شده و منتقل شده را رمزگذاری نمی‌کنند، و هکرها بسیار آسان میتوانند به این اطلاعات دسترسی پیدا کنند. نظارت بر حقوق مصرف کننده چه کرد؟ این دستگاه ها را به لحاظ امنیتی "ضعیف" نامید و افزود اگر والدین از آسیب پذیری‌هایی امنیتی که در این دستگاه‌ها وجود دارد اطلاع پیدا کنند "شوکه" خواهند شد.

ساعت‌های Gator 2، Tinitell، Viksfjord و Xplora آزمایش شدند، اما محققان می‌گویند محصولات دیگر می‌توانند آسیب پذیر باشند. جان لوئیس، خرده فروش انگلیسی اعلام کرده است در حال ارائه "مشاوره بیشتر و اطمینان به عرضه کننده" نسخه دیگری از ساعت Gator را در یک اقدام محتاطانه از لیست فروش خود حذف کرده است.

GPS برای کودکان اعلام کرد که در حال حاضر به نقص امنیتی واقف هست، به مشتریان خود قول داد که نقص موجود را ارتقا می‌دهد. در عین حال، Gator گفته است که داده‌هایش را به یک سرور جدید رمزگذاری شده انتقال داده است و یک برنامه امن‌تر را برای مشتریانش ایجاد کرده است.

محصولات مصرفی به طور فزاینده‌ای به اینترنت متصل می‌شوند در نتیجه سطح بی-سابقه‌ای از داده‌ها تولید، جمع‌آوری و پردازش می‌شوند. ضروری است که از تهدیداتی که ممکن است چنین محصولاتی را درگیر کند آگاه باشیم، اگر امنیت در اولویت قرار گیرد. هریسون ادوارد شن، معاون ارشد ارزیابی امنیتی فنی، گفت: "ما شورای مصرف کننده نروژ را متقاعد کردیم که روند پیگیری این امر حرکت رو به جلو داشته باشد"

گردآورنده: سمیه نیاخلیلی

معرفی سرویس امنیتی جدید گوگل برای دفع حملات سایبری

همزمان با تحقیقات امنیتی در حال انجام در روسیه پیرامون آسیب پذیری گسترده Equifax، گوگل در حال معرفی سرویس جدیدی است که امنیت سیستم احراز هویت دو مرحله ای را بهبود می‌بخشد، البته ممکن است این سرویس برای همه کاربران قابل دسترس نباشد.

به گفته دو تن از افراد آگاه به این موضوع و بنابر گزارش بلومبرگ، گوگل برنامه امنیتی پیشرفته‌اش را در ماه آینده به بازار عرضه خواهد کرد. مشتریان این محصول، عمدتاً مدیران شرکت‌های بزرگ، سیاستمداران و دیگر شخصیت‌های برجسته‌ای هستند که الزامات امنیتی شدیدی دارند. این که آیا این سرویس برای کاربران عادی در دسترس خواهد بود، نامشخص است.

گوگل از سال ۲۰۱۴ پشتیبانی از کلیدهای امنیتی USB موسوم به U2F را از سر گرفت. (فیس بوک، Dropbox و Salesforce قبل از گوگل از این تکنولوژی پشتیبانی می‌کردند). این تکنولوژی، امنیت حساب‌های کاربری گوگل مانند Gmail را با اتصال یک دانگل USB به رایانه - با ورود یک رمز عبور استاندارد - بهبود می‌بخشد. در این روش دیگر نیازی به تایپ کدها از تلفن همراه نیست و همچنین کاربر از سایت‌های فیشینگ بیشتر در امان می‌ماند.

الگوی امنیتی جدید گوگل بر پایه همین روش است با این تفاوت که کلید سخت افزاری فیزیکی دومی علاوه بر کلید امنیتی USB، مورد استفاده قرار می‌گیرد. به این صورت که تنها زمانی وارد یک حساب Google خواهیم شد که هر دو دستگاه (کلید) شناسایی شوند.

نوآوری‌های این طرح امنیتی به اینجا ختم نمی‌شود. این سرویس علاوه بر اینکه دسترسی تمامی برنامه‌های شخص ثالث را به فایل‌های Google Drive مشتری مسدود می‌کند، بلکه به روز رسانی‌های امنیتی منظمی را برای حفظ امنیت اطلاعات با استفاده از به روز ترین روش‌ها، ارائه می‌دهد.

اخیراً مشخص شد که غول حسابداری Deloitte شرکت دیگری بود که قربانی هکرها شد. سرور ایمیل اصلی این شرکت، از طریق یک حساب کاربری مدیر در معرض خطر قرار گرفت که تنها با یک کلمه عبور محافظت شده بود و از سیستم احراز هویت دو مرحله‌ای استفاده نمی‌کرد.

گردآورنده: محمدحسین خدامی

باج افزار BadRabbit

نسل جدیدی از باج افزار به نام "خرگوش بد" در روسیه، اوکراین و سایر بخش‌های شرقی اروپا در حال گسترش می‌باشد. به نظر می‌رسد که علارغم شباهت‌های موجود با باج افزار Petya اما از آن متفاوت می‌باشد. از این رو این باج افزار توانسته است باعث ویرانی در سیستم رسانه‌ای، حمل و نقل عمومی و یک فرودگاه در اکراین گردد.

همانند سایر باج افزارها "خرگوش بد" نیز توانسته است از طریق یک فایل Flash جعلی گسترش پیدا کند، اما این باج افزار این قابلیت را دارد که توسط شبکه گسترش یابد و سیستم‌های بیشتری را آلوده نماید. گسترش باج افزار با استفاده از کد متن باز Mimikatz برای استخراج اعتبارنامه‌ها و DiskCrypt برای رمزنگاری داده‌ها بسیار تسهیل گردیده است.

شیوع گسترش خرگوش بد به عنوان یک حمله مداوم توصیف گردیده است و مرکز CERT مربوط به اوکراین آگاهی‌ها لازم را به شرکت‌ها در خصوص این باج افزار داده است. زمانی که محتوای هارد رمزنگاری شد، این باج افزار با جابه جایی MBR باعث دسترسی ناپذیری آن می‌گردد.

پیغام این باج افزار بسیار شبیه به پیغام باج افزار NotPetya می‌باشد و بررسی‌ها نشان می‌دهد که مقداری از کد منبع آن نیز مجدد مورد استفاده قرار گرفته است. شرکت ESET نیز همچنین اعلام نمود که شرکت‌های زیادی در شرق اروپا به این باج افزار آلوده شده‌اند. شرکت Micro Trend همچنین بیان نمود: "براساس تحقیقات ما، باج افزار خرگوش بد قابلیت گسترش خود را برروی سایر کامپیوترهای موجود در شبکه و کپی کردن فایل‌های خود در شبکه با استفاده از نام اصلیشان و همچنین اجرای کپی‌های ایجاد شده را با استفاده از Windows Management Instrumentation (WMI) و Service Control Manager Remote Protocol را دارد."

درحالی که مقدار باج درخواستی ۰.۰۵ بیت کوین است اما مرکز CERT این هشدار را داده است که با پرداخت مبلغ باج هیچ ضمانتی برای بازگشت فایل‌ها و رمزگشایی وجود ندارد.

راه مقابه با این باج افزار

با این که هدف این باج افزار شرق اروپا می‌باشد اما نمونه‌هایی از آن نیز در امریکا مشاهده شده است. خوشبختانه با استفاده از چند راه حل ساده می‌توان جلوی فعالیت این باج افزار را گرفت.

راه حل پیشنهادی از سوی یک محقق امنیتی به نام Amit Serper در توییتر ارائه گردیده است. تمام کاری که نیاز است انجام دهید ایجاد دو فایل c:\windows\infpub.dat و c:\windows\cscc.dat می‌باشد. سپس نیاز است تا تمامی دسترسی‌های حذف گردد. این کار باعث می‌شود شما در مقابل

این باج‌افزار واکسینه شوید و این باج افزار نتواند در سیستم شما فعالیت کند.

راه حل پیشنهادی از سوی Kaspersky غیرفعال کردن WMI است تا از گسترش این باج افزار جلوگیری شود. برای غیرفعال سازی WMI به صورت زیر باید عمل نمود:

در Run عبارت Services.msc را تایپ نموده و Ok را فشار دهید.

برروی Windows Management Instrumentations کلیک راست نموده و Properties را انتخاب نمایید.

برروی دکمه‌ی Stop کلیک کرده و از لیست کشویی Startup type مقدار Disabled را انتخاب و برروی Ok کلیک کنید.

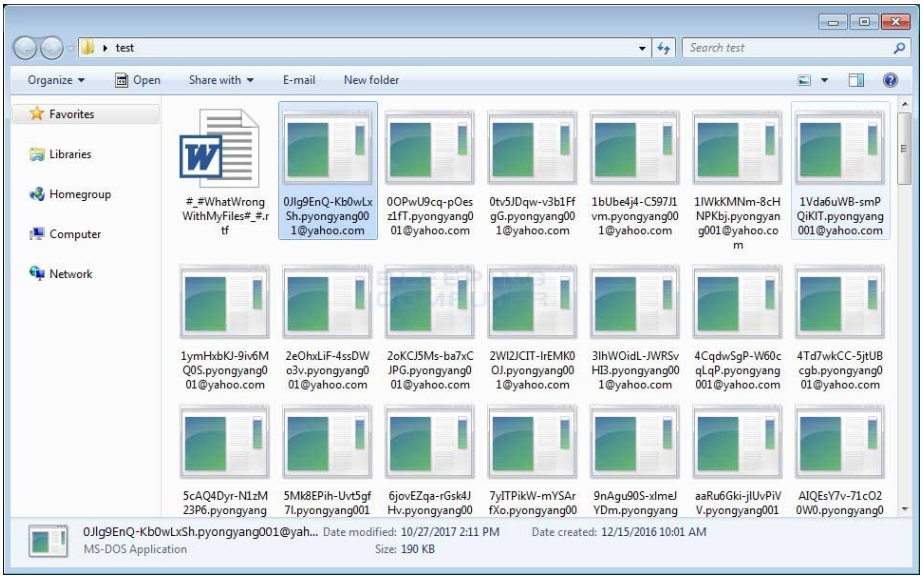
گردآورنده: محمد مرتضوی

بازگشت دوباره باج افزار Matrix

محقق امنیتی شرکت Malwarebytes به نام Jérôme Segura دریافته است که باج افزار ماتریکس با استفاده از کیت اکسپلویت RIG برروی سایت‌هایی که میزبان بدافزارهای تبلیغاتی هستند مجددا در حال گسترش می‌باشد.

باج افزار ماتریکس اولین بار در انتهای سال ۲۰۱۶ انتشار یافت و در ماه آپریل سال ۲۰۱۷ شناسایی گردید. از آن زمان به بعد سرعت این گسترش کاهش یافت و تنها در نقاط کمی مشاهده گردید. بنابراین، خبر گسترش دوباره‌ی آن توسط کیت اکسپلویت RIG همه را شوکه کرد.

برطبق بیانات Segura، باج افزار ماتریکس از طریق این کیت و با استفاده از سایت‌هایی که تبلیغات مخرب به نمایش می‌گذارند برروی اهدافی که دارای آسیب پذیری‌های CVE-2016-0189 در Internet Explorer و CVE-2015-8651 در Flash باشند نصب می‌گردد. هر دوی این آسیب پذیری‌ها به کاربرانی مربوط است که از نسخه‌های آپدیت نشده و قدیمی Internet Explorer و Flash Player استفاده می‌کنند.

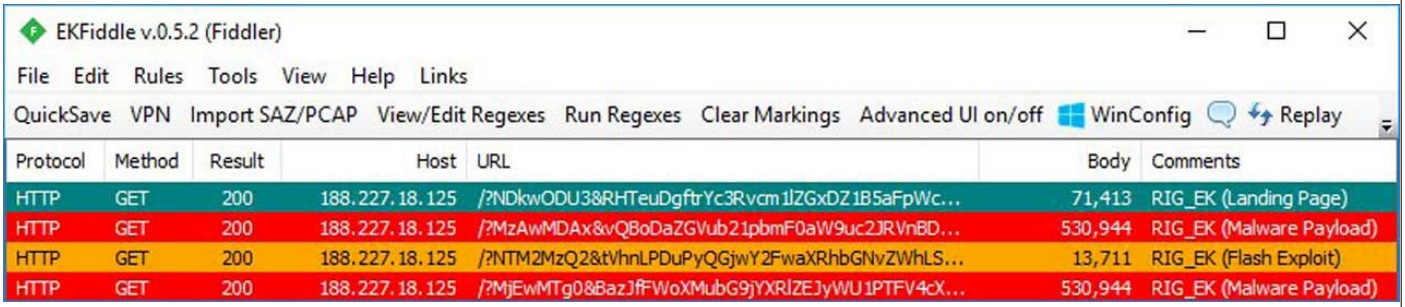


برای آلوده شدن کافیست که تنها بازدید کننده با استفاده از یک سیستم آسیب پذیر وارد سایت‌هایی شود که تبلیغات مخرب و آلوده به نمایش می‌گذارند. این دلیلی قانع کننده بر این امر است که کاربران باید به صورت دوره‌ای آپدیت‌های مورد نیاز را دریافت و نصب نمایند.

به محض اینکه فرد آلوده شود، تمام فایل-های آن برروی کامپیوتر رمزنگاری می‌گردد، نام آنان تغییر پیدا می‌کند و به فرمت آنان به pyongyan001@yahoo.com تغییر پیدا می‌کند.

در طول این فرآیند، باج افزار یک فایل نوشته را در تمامی فولدرهایی که رمزنگاری کرده است با نام WhatWrongWithMyFiles#_#.rtf قرار می‌دهد. سرانجام یک صفحه که توضیحات کاملی در خصوص شرایط برقراری ارتباط و پرداخت باج در آن نوشته شده است نمایش داده می‌شود.

ادامه در صفحه بعد.



گردآورنده: محمد مرتضوی

بازگشت دوباره باج افزار Matrix (ادامه...)

اما راهکارهای متفاوتی نیز برای جلوگیری از آلوده شدن به این باج افزار نیز ارائه گردیده است که در ادامه به آنان خواهیم پرداخت.

چگونه خود را از آلوده شدن به این باج افزار دوره نگه داریم؟

در ابتدا نیاز است تا از نصب تمامی آپدیت-های امنیتی ویندوز خود مطمئن شویم. این امر مانع از اجرای کیت Exploit برروی سیستم ما خواهد شد.

همچنین استفاده از یک نرم افزار امنیتی خوب بسیار مهم می‌باشد. برای شروع باید یک پشتیبان قابل اعتماد و آزمایش شده از داده‌های خود داشته باشید که در موارد اضطراری و در هنگام حمله باج افزار بتوان فایل‌ها را از آن بازگردانی کرد.

همچنین شما باید مجهز به سیستم‌های امنیتی تشخیص رفتاری همانند Malwarebytes و یا Emsisoft Anti-Malware باشید. اگر از آپدیت Fall Creater ویندوز ۱۰ استفاده می‌کنید لازم است تا ویژگی Controlled Folder Access را برای محافظت از فایل‌هایتان در مقابل باج افزارها، فعال نمایید.

در آخر رفتارهای امنیتی مناسب را تمرین کنید. این رفتارها به صورت خلاصه شامل گام‌های زیر می‌شود:

- تهیه‌ی نسخه‌ی پشتیبان.
- باز نکردن پیوست ایمیل‌هایی که از سوی افراد ناشناس ارسال شده‌اند.
- اسکن فایل‌های پیوست ایمیل‌ها با استفاده از آنتی ویروس.
- اطمینان از نصب به روز رسانی‌های ویندوز به محض انتشار آنان. همچنین سعی کنید تا تمامی برنامه‌های خود را به روز نگه دارید به خصوص Java، Flash و Adobe Reader. نسخه-های قدیمی برنامه‌ها دارای آسیب پذیری‌هایی می‌باشد که بدافزارها برای گسترش از آنان سوء استفاده می‌کنند.
- استفاده از نرم فزارهای امنیتی مناسب.
- از پسوردهای پیچیده در وب سایت‌ها استفاده نمایید. همچنین از یک پسورد در چندین سایت استفاده نکنید.

همچنین ذکر این نکته در انتها مناسب ایت که جلوگیری از آلوده شدن به این باج افزارها بسیار ساده‌تر از بازگرداندن فایل‌های رمزنگاری شده پس از آلودگی می‌باشد.

گردآورنده: محمد مرتضوی

هک آیفون ۷ توسط Pwn2Own

امنیت آیفون ۷ توسط یک گروه سه نفره از هکرها در رویداد موبایل Pwn2Own با استفاده از یک آسیب پذیری در wi-fi، یک باگ در سیستم خدمات و دو باگ در Safari به مخاطره افتاد و هکرها توانستند کدهای مخرب خود را برروی دستگاه مورد نظر با استفاده از این آسیب پذیری‌های روز صفر اجرا نمایند.

آزمایشگاه امنیتی Tencent Keen در دو بخش از سه بخش مربوط به کنفرانس Pwn2Own با استفاده از دو باگ در Safari مربوط به آیفون ۷ موفق به گریز از SandBox شد. در حال حاضر همچنان این حمله توسط رهبران Pwn2Own تایید نگردیده است.

قوانین مسابقه تاکید بر این امر دارد که تمامی دستگاه‌هایی که تحت نفوذ قرار می‌گیرند باید به آخرین نسخه سیستم عامل آپدیت شده باشند و تمامی Patch های امنیتی را دریافت کرده باشند. دقیقا مشخص نیست در دقیقا در آن روز چه نسخه‌ای از iOS برروی آیفون ۷ نصب گردیده شده بود. سه شنبه Patch مربوط به آسیب پذیری KRACK برای iOS 11.1 منتشر گردید که برای سوء استفاده از wi-fi استفاده می‌گردد.

هنگامی که تحقیقات ارائه شده نشان داد که این آسیب پذیری 0-day است، Pwn2Own بلافاصله این آسیب پذیری را به فروشندگان ارائه داد. تیم هک کننده ۴۵۰۰۰ دلار به علاوه‌ی ۱۲ امتیاز دریافت کردند. به آنان یک فرصت ۹۰ روزه داده می‌شود تا یک راه حل قبل از آنکه شرکت درباره این متد "توصیه‌های محدودی" ارائه کند را منتشر کنند. نمایندگان گوگل، اپل و هوآوی در محل این کنفرانس حاضر هستند و می‌توانند در صورت نیاز سوالاتشان را مطرح نمایند.

یک باگ در مرورگر اینترنت سامسونگ در این رویداد نیز کشف گردید. گوشی سامسونگ مربوطه Galaxy S8 می‌باشد. همچنین آزمایشگاه امنیتی Keen از روش Stack Overflow برای نفوذ به گوشی Huawei Mate9 Pro و اجرای کدهای مخرب استفاده نمود که با این کار ۱۰۰۰۰۰ دلار به دست آورد.

Pwn2Own یک مسابقه‌ی کامپیوتری هک می‌باشد که افتتاحیه‌ی آن در سال ۲۰۰۷ بوده و هرساله برگزار می‌گردد. اولین مسابقه درخصوص فقدان پاسخگویی اپل به Month of Apple Bugs و Month of Kernel Bugs برگزار شد. در آن زمان رویدادها و همچنین آگهی‌های بازرگانی اپل، امنیت ویندوز را به تمسخر گرفته بودند.

برنده‌ی این مسابقه، گوشی موبایلی که با آن حمله را انجام داده، پول نقد و یک ژاکت مربوط به مسابقات را دریافت می‌کند. مکان آخرین رویداد نام برده در خیابان Aoyama و در Grace Cathedral در توکیو ژاپن برگذار گردید.

گردآورنده: محمد مرتضوی

باگ در DNS ویندوز

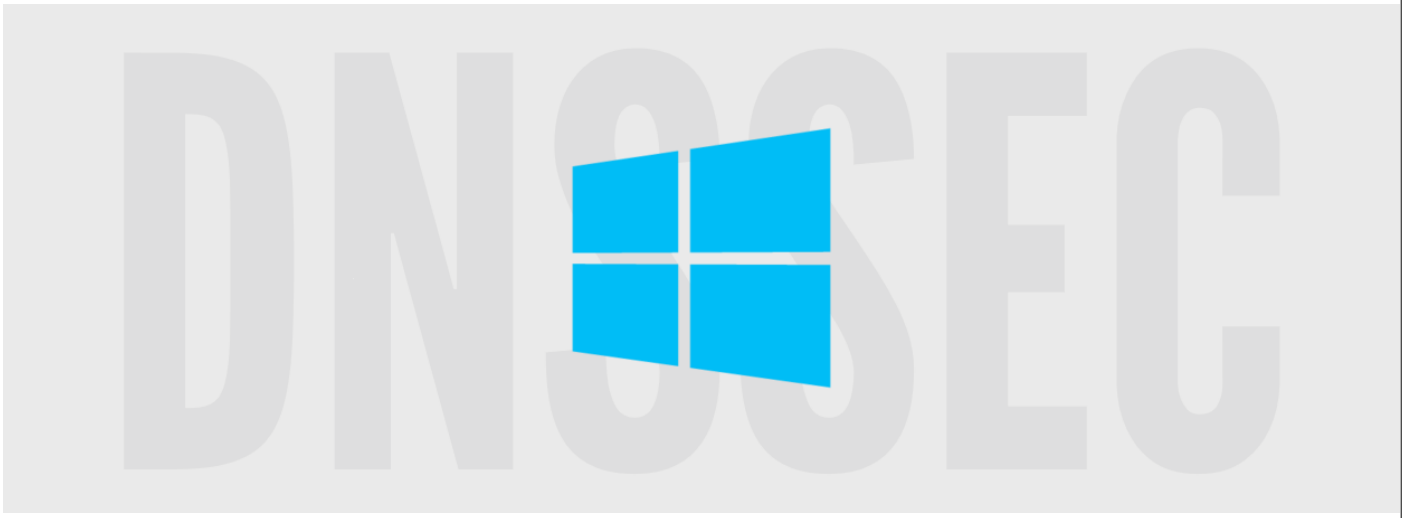
در سرویس DNS ویندوز ۸، ویندوز ۱۰، ویندوز سرور ۲۰۱۲ و ویندوز سرور ۲۰۱۶ ، باگی که با شناسه CVE-2017-11779 ردیابی شده است – یافت شده که روی DNSAPI.dll اثر می‌گذارد. DNSAPI.dll فایل است که درخواست های DNS را می‌سازد و پاسخ را از سرور DNS دریافت می‌کند. این باگ فقط به ویندوز ۸ یا بالاتر اختصاص دارد زیرا نقص امنیتی در چگونگی اجرای فایل DNSAPI.dll و مدیریت درخواست‌های DNS ساخته شده در حین پروتکل DNSSEC را وجود دارد. DNSAPI یک ورژن امن تر از پروتکل کلاسیک DNS است. ویندوز ۸ اولین نسخه ویندوز برای پشتیبانی از این پروتکل بود.

باگ شرایط اجرای کد مخرب با سطح دسترسی مدیرسیستم را فراهم می‌کند.

Nick Freeman، محقق امنیتی BishopFox کشف شده می‌گوید: برای بهره برداری از باگ، مهاجم باید یک سرور DNS مخرب را راه اندازی کند و شبکه‌ی محلی هدف را برای ربودن ترافیک DNS از بین ببرد. در آن نقطه مهاجم تنها به انتظار برای یک برنامه با ادمین یا system-level privileges برای ساخت درخواست DNS نیاز دارد. این مسئله ای نیست چون بسیاری از برنامه های امروزی درخواست-های DNS را مهیا می‌سازند و بسیاری از کاربران از یک اکانت Windows admin -level برای عملیات روز به روز خود استفاده می‌کنند. علاوه بر این، DLL مشابه هم درخواست‌های DNS ساخته شده توسط بسیاری از سرویس‌های ویندوز اصلی را انجام می‌دهد، بنابراین، مهاجم در نهایت پاسخ DNS مورد نظرخود را توسط یک از سرویس های اصلی دارد، که کد مخرب اضافه شده در درون را با system-level privileges اجرا می‌کند. محققان توضیح می‌دهند که سرویس Windows DNS caching که فایل DNSAPI.dll را استفاده می‌کند اگر درهم بشکند، به صورت اتوماتیک ری استارت خواهد شد. این باعث می‌شود که مهاجم تلاش های نامحدودی برای بهره برداری از باگ تا زمانی که دسترسی به سطح سیستم را به دست آورد، داشته باشد.

مهاجم نیاز به مسیر مستقیمی برای اهداف دارد.

تنها خبر خوب برای کاربران این است که بسته‌های DNS آلوده برای استفاده از این باگ نباید از سرورهای DNS قانونی عبور کنند. این بدان معناست که مهاجم باید با هدف خود روی شبکه باشد. مایکروسافت این باگ را با آپدیت بخشی از the October 2017 Patch Tuesday که امروز منتشر شده، به روز رسانی کرد.



گردآورنده: حسین علیمرادی

پچ آسیب پذیری‌های KRACK WPA2 در اندروید

گوگل پچ لازم برای رفع آسیب پذیری KRACK که در ماه گذشته منتشر شد را فراهم نمود. آگهی امنیتی اندروید در نوامبر ۲۰۱۷ به سه بخش جداگانه تقسیم شده است: ۰۱-۱۱-۲۰۱۷ و۰۵-۱۱-۲۰۱۷ و ۰۶-۱۱-۲۰۱۷. اصلاحات کرک در تاریخ دوم (۰۶-۱۱-۲۰۱۷) قرار دارد. اگر گوشی شما به روزرسانی را دریافت کرده و سطح پچ امنیتی آن تا تاریخ ۰۶-۱۱-۲۰۱۷ باشد؛ اصلاح کرک نیز در آن قرارداده شده است. MathyVanhoef، محقق دانشگاه لووان (KULeuven) ، اظهار داشت که آسیب پذیری کرک بر روی پروتکل WiFi WPA2 تاثیر می گذارد و اجازه می دهد تا مهاجمان کنترل کلید های اتصال مجدد نصب و ترافیک WiFiمحافظت شده توسط WPA2را به دست بگیرند. هنگامی که وانوئوف پژوهش خود را به صورت عمومی انتشار داد؛ شرکت های بزرگ برای محصولات خود پچ مناسب را ارائه دادند. گوگل یکی از آخرین فروشندگان عمده برای ارائه اصلاحات کرک بود. در مقایسه با مایکروسافت که رفع کرک را به کاربران ویندوز ، یک ماه قبل از آسیب پذیری اطلاع رسانی کرده بود. اپل قسمت هایی از کرک را در اواخر اکتبر به عنوان بخشی از iOS 11.1 و macOS High Sierra 10.13.1 منتشر کرد. کاربران می توانند دستگاه های آسیب پذیر به حملات کرک را با ابزار و کد اثبات مفهوم شناسایی کنند.ازطریق کد وانهوف که از طریق حساب GitHub خود او منتشر شده است و یا از طریق این ابزار جانبی توسعه یافته شخص ثالث به نامKRACK Detector.

اشکالات دیگر که در آگهی امنیتی Android 2017 تایید شده است

علاوه بر رفع کرک، گوگل همچنین دیگر نقص های امنیتی را به عنوان بخشی از آگهی امنیتی Android 2017 انتخاب کرده است. این مورد شامل پنج اشکال راه اندازی کد است که اجازه می دهد تا مهاجمان از طریق فایل های چندرسانه ای (CVE-2017-0832، CVE-2017-0833، CVE-2017-0834، CVE-2017-0835، CVE-2017-0836) به اجرای بدافزار مدنظر خود نائل شوند. علاوه بر این، آگهی امنیتی شامل رفع شش نقص گزارش شده توسط محقق امنیتی اسکات بئور می باشد. نقص های امنیتی مذکور بر Qualcomm WLAN تاثیر می گذارند . جزئیات بیشتر در و وب سایت Bauer که به طور خاص برای این منظور راه اندازی شده است توضیح داده شده است .

گردآورنده: حسین علیمرادی

MineCraft و سرقت اطلاعات کاربران!

بر طبق تحقیقات محققان امنیتی Symantec بازی Minecraft با میلیون بازی کننده فرصت جدیدی است که جنایتکاران سایبری به آن دست یافته‌اند. Shaun Aimoto مهندس تضمین کیفیت نرم افزار در وبلاگ شرکت گزارش کرده است که Mod دست ساز Minecraft به نام Pocket Edition در حال ربودن اطلاعات تبلت‌ها و گوشی‌های هوشمند برای یک Botnet تبلیغاتی است.

بیش از ۵۵ میلیون نفر مرد، زن و بچه بازی Minecraft را به طور میانگین در ماه بازی می‌کنند. خیلی از این افراد از استفاده کردن ابزار شخص ثالث "mods" برای شخصی سازی بیشتر در این بازی لذت می‌برند. استفاده از mods های مختلف عناصر بازی Minecraft را برای کودکان تغییر می‌دهد. اغلب این تغییرات ساده برای ظاهر بازی صورت می‌گیرد (فرآیندی که به آن پوسته گفته می‌شود). زمانی که ۵۵ میلیون نفر در حال انجام بازی هستند که می‌توانند دنیای دیجیتال خود را بسازند، انتظار می‌رود که آنان نشان شخصی خود را نیز برای آواتارشان داشته باشند.

بر طبق تحقیقات محققان امنیتی Symantec این بستر فرصت جدیدی است که جنایتکاران سایبری به آن دست یافته‌اند.

Shaun Aimoto مهندس تضمین کیفیت نرم افزار در وبلاگ شرکت گزارش کرده است که مد دست ساز Minecraft به نام Pocket Edition در حال ربودن اطلاعات تبلت‌ها و گوشی‌های هوشمند برای یک Botnet تبلیغاتی است.

بر طبق گفته‌های Aimoto، بدافزارها توسط Google Play Store با عنوان پوسته در حال گسترش هستند. بر اساس مشاهدات، Symantec معتقد است که چیزی در حدود ۶۰۰۰۰۰ تا ۲.۵ میلیون بازیکن Minecraft این اپلیکیشن‌های مشکوک را نصب نموده‌اند.

هدف اولیه از تولید بدافزارهای موبایلی، کسب درآمد از طریق تولید آگهی‌های جعلی می‌باشد. هرچند که ممکن است این امر باعث ایجاد خطرات جدی‌تری در آینده گردد. به دلیل گسترش سریع و اجرای این بدافزار برروی دیوایس‌های فراوان و دسترسی آنان به اینترنت، این بدافزار به صورت بالقوه امکان انجام حملات DDoS را دارد.

گیمرها عموما به دلیل داشتن حرکات فوق العاده خطرناک، هدف مهاجمان اینترنتی قرار می‌گیرند. برخی از این حرکات عبارتند از ایجاد پول و اعتبار رایگان در بازی و همچنین حذف محافظت از نسخه‌های کپی می‌باشد. هکرها از طریق نسخه‌های آلوده و به اصطلاح بمب گذاری شده از بازی که در سطح اینترنت به اشتراک می‌گذارند قربانیان را آلوده می‌کنند.

مجرمان اینترنتی می‌دانند که گیمرها عموما افراد جوانی هستند که نمی‌دانند شخصی در گوشه‌ای از اینترنت برای طعمه قرار دادن آنان در کمین نشسته است.

شرکت Symantec بیان می‌کند که نصب یک اسکن کننده‌ی بدافزار برروی وسایل دیجیتالی و آپدیت بودن آن، چک کردن اجازه‌های دسترسی اپلیکیشن‌ها قبل از نصب راهکارهایی برای جلوگیری از این خطرات هستند. یک اپلیکیشن پوسته‌ی ساده از بازی Minecraft هیچ گاه به اطلاعات مکانی شما نیاز پیدا نخواهد کرد. پس باید در خصوص این دسترسی‌ها بسیار آگاه بود.

گردآورنده: محمد مرتضوی

Kharazmi CERT Coordinator Center

مرکز آپا دانشگاه خوارزمی

رییس مرکز:

دکتر امید مهدی عبادتی

اعضای هیات علمی:

دکتر احسان ملکیان

دکتر امید مهدی عبادتی

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

محسن یزدی نژاد

نشانی:

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

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

پست الکترونیک:

cert@khu.ac.ir

وب سایت:

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

دانلود رایگان:

دانلود رایگان مجموعه کامل خبرنامه‌ها