شماره نهم - مهر ۱۳۹۶

خبرنامه "آپا" دانشگاه خوارزمی

در این شماره خواهید خواند:

آیا آنتی ویروس DU از موبایل شما محافظت می‌کند؟

محققان شرکت چک پوینت، اخیرا یک برنامه آنتی ویروس موبایل رایگان توسعه یافته توسط گروه DU که اطلاعات کاربر را بدون رضایت صاحبان دستگاه جمع آوری می‌کند، - صفحه ۲ و ۳

- **چه اپلیکیشن‌هایی از اندروید و iOS اغلب توسط شرکت‌ها در لیست سیاه ثبت شده‌اند؟**

براساس اطلاعات جمع آوری شده توسط Appthority، برنامه‌ها معمولا به دلیل این واقعیت که داده‌ها را از بین می‌برند؛ به لیست سیاه اضافه می‌شوند. - صفحه ۶

آغازی برای Bashware

محققان امنیتی می‌گویند که در WSL راهی برای اجازه دادن به بدافزارها برای نقض آنتی ویروس‌ها پیدا کرده‌اند. - صفحه ۹

پیشنهاد جدید اینتل برای کمک به ایمن سازی خودکار دستگاه‌های اینترنت اشیاء

محصول جدید اینتل به نام Intel Secure Device Onboard (Intel SDO)، به عنوان یک سرویس به ارائه دهندگان پلت فرم‌های IoT ارائه خواهد شد تا در سریع‌ترین زمان ممکن راهکاری برای نصب بسته‌های به روز رسانی و مدیریت هزاران دستگاه متصل را ارائه دهند. - صفحه ۴

یک ابزار تجزیه و تحلیل جدید از مایکروسافت برای مهندسان امنیت و توسعه دهندگان!

این ابزار که VulnScan نامیده می‌شود، توسط مرکز پاسخگویی امنیتی مایکروسافت (MSRC) طراحی و توسعه یافته است تا به تعیین نوع آسیب پذیری و علت اصلی نقص های فیزیکی حافظه کمک کند. - صفحه ۷

یاهو: ۳ میلیارد حساب کاربری از سال ۲۰۱۳ در معرض خطر است

به نظر می‌رسید ۱ میلیارد نفر از این نقض امنیتی تحت تاثیر قرار گرفته‌اند اما این تعداد همچنان افزایش می‌یابد. بیش از ۳ میلیارد نفر ممکن است تحت تاثیر این نقص قرار گیرند. - صفحه ۵

باج افزاری به نام RedBoot

این باج افزار نه تنها فایل‌ها را رمزنگاری می‌کند، بلکه قادر به تغییر جدول پارتیشن و مستر بوت ریکورد (MBR)می‌باشد که به نظر می‌رسد این امر باعث آسیب دائمی خواهد گردید. - صفحه ۸

- **۱۰ آسیب پذیری مهم در D-Link**

پیر کیم، یکی از محققان امنیتی، تصمیم گرفت تا عموم آسیب پذیری‌های مربوط به روترهای D-Link 850L را در معرض عموم قرار دهد. - صفحه ۱۰ و ۱۱

آیا آنتی ویروس DU از موبایل شما محافظت می‌کند؟

در طول نیمه‌ی اول سال ۲۰۱۷، حملات موبایلی نزدیک به ۲۰ درصد از تمام حملات سایبری در آمریکا را شکل می‌دهد. کارشناسان به طور مداوم به کاربران در مورد خطرات ناشی از نصب نرم افزار امنیتی برای محافظت از دستگاهایشان هشدار داده‌اند. اما زمانی که آنتی ویروسی قابل اعتماد نیست و در واقع حریم خصوصی کاربران را به خطر می اندازد، چه اتفاقی خواهد افتاد؟

محققان شرکت چک پوینت، اخیرا یک برنامه آنتی ویروس موبایل رایگان توسعه یافته توسط گروه DU (توسعه دهنده برنامه‌های اندروید) که اطلاعات کاربر را بدون رضایت صاحبان دستگاه جمع آوری می‌کند، کشف کرده‌اند. اپلیکیشن DU Antivirus Security بر روی Google Play، توزیع شده و بین ۱۰ تا ۵۰ میلیون بار دانلود شده است.

براساس تحقیقات چک پوینت، زمانی که برنامه برای اولین بار اجرا می‌شود اطلاعاتی مثل شناسه‌های منحصربه فرد، لیست مخاطبین، لیست تماس‌ها و حتی موقعیت دستگاه را جمع آوری می‌شوند. سپس این اطلاعات رمزگذاری شده و به یک سرور فرستاده می‌شود. اطلاعات کاربران همچنین بعدا توسط یک برنامه دیگر ارائه شده توسط گروه DU به نام "Call - Caller ID Block - DU Caller" مورد سو استفاده قرار می‌گرفت.

این آنتی ویروس اطلاعات شخصی کاربرانش

را بدون اجازه جمع کرده و از این اطلاعات خصوصی برای اهداف تجاری خود استفاده می‌کند. اطلاعاتی در مورد تماس‌های شخصی، اینکه با چه کسی صحبت می‌کنید و چه اندازه این تماس‌ها طول می‌کشد.

چک پوینت، استفاده‌ی غیرقانونی از اطلاعات خصوصی کاربران را در ۲۱ آگوست ۲۰۱۷ گزارش کرد و برنامه در ۲۴ آگوست ۲۰۱۷ از گوگل پلی حذف شد. ورژن جدید این آنتی ویروس که کد مخرب ندارد در ۲۸ آگوست در پلی استور آپلود شد. ورژن شماره‌ی ۳.۱.۵ از DU Antivirus Security آخرین شماره‌ی ورژن یافت شده است که در بردارنده‌ی کد ناقض حریم خصوصی است اما ورژن‌های قدیمی‌تر ممکن است هنوز این کد مخرب را داشته باشند.

علاوه بر DU Antivirus Security، محققان چک پوینت چنین کدی را در ۳۰ اپ دیگر از برنامه‌های گوگل پلی پیدا کردند و متعاقبا آن اپلیکیشن‌ها را از گوگل پلی حذف کردند. این برنامه‌ها احتمالا کد را به عنوان یک کتابخانه خارجی اجرا کرده و داده‌های سرقت شده را به همان سرور راه دور که توسط DU Caller مورد استفاده قرار می‌گیرد، انتقال می‌دادند. در مجموع، طبق داده‌های Google Play، بین ۲۴ تا ۸۹ میلیون قربانی این برنامه‌ها را نصب کرده‌اند.

کاربرانی که DU Antivirus Security یا هر اپ دیگری را نصب کرده اند باید برنامه‌هایشان را توسط آپگرید به آخرین ورژنی که این کد مخرب را ندارد مورد بازبینی قرار دهند.

از آنجاییکه برنامه‌های آنتی ویروس دلیلی موجه برای درخواست مجوزهای غیرمعمول دارند، پوششی مناسب برای متقلبانی هستند که به دنبال سوء استفاده از این مجوزها هستند.

ادامه در صفحه بعد.

گردآورنده: حسین علیمرادی

آیا آنتی ویروس DU از موبایل شما محافظت می‌کند؟ (ادامه...)

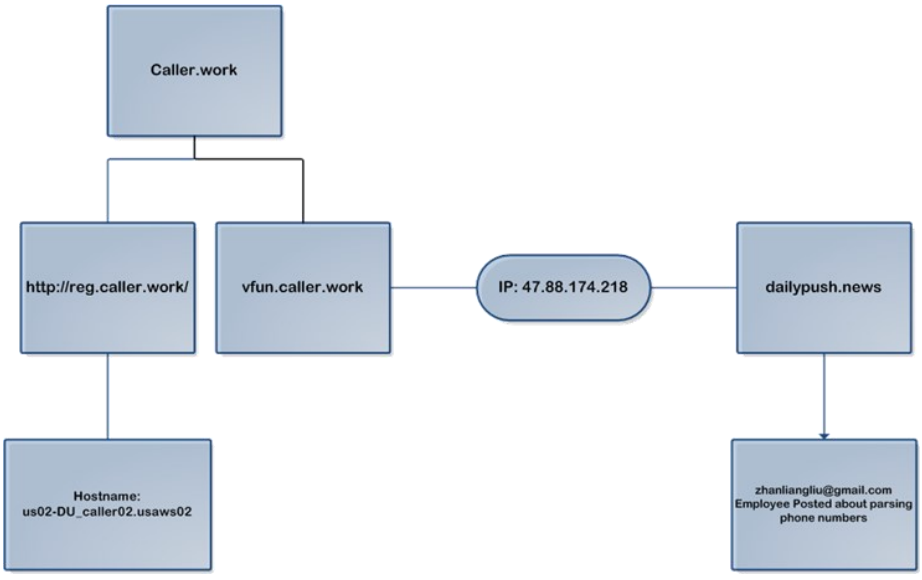
در بسیاری از موارد اپ‌های آنتی ویروس موبایل حتی به عنوان یک دام برای تحویل بدافزار استفاده می‌شوند. کاربران باید از این آنتی ویروس‌های مشکوک آگاه باشند و تنها از آنتی ویروس‌هایی استفاده کنند که توسط فروشندگان معتبر ارائه می شوند که اثبات شده قادر به محافظت از دستگاه‌های تلفن همراه و داده‌های ذخیره شده در آن‌ها هستند.

جزئیات تکنیکی

DU Antivirus Security وقتی که برای اولین بار اجرا می شود، اطلاعات را از دستگاه کاربران به سرقت می‌برد. اطلاعات به سرقت رفته به سرور caller.work که در اپ‌های DU به ثبت نرسیده است منتقل خواهد شد. این دامنه دارای دو زیر دامنه است که نشان می‌دهد به برنامه DU caller متصل است. اولین زیر دامنه http://reg.caller.work/ است. که یک صفحه‌ی PHP می‌باشد که hostname خود را اینطور مشخص می‌کند: us02-Du_caller02.usaws02 و در برداردنده‌ی نام اپ DU caller است.

علاوه بر این، زیر دامنه‌ی vfun.caller.work که روی آی پی ۴۷.۸۸.۱۷۴.۲۱۸ هاست شده است، یک سرور خصوصی می‌باشد که هاست دامنه‌ی dailypush.news نیز می‌باشد. این دامنه با zhanliangliu@gmail.com که کارمند Baidu است، ثبت شده و از همان آدرس ایمیل برای پست کردن تجزیه تحلیل‌های شماره تلفن (http://zliu.org/post/python-libphonenumber/) استفاده شده است. چون اپلیکیشن‌های DU قسمتی از گروه Baidu هستند و پست مربوط به یک قابلیت مربوط به caller app است، نشان دهنده‌ی یک ارتباط بین اطلاعات به سرقت رفته و caller app است.

برنامه DU caller در حال حاضر برای سیاست‌های حفظ حریم خصوصی مبهم، که شرایط مختلف را در صفحات جداگانه نمایش می‌دهد. اجرای فعالیت‌هایی بدون در نظر گرفتن رضایت کاربران باعث شده این شرکت تحت فشار قرار بگیرد. سال گذشته، آنتی ویروس Cheetah Mobile بعد از ارائه‌ی یک سرویس که ممکن بود مقررات حفظ حریم خصوصی را نقض کند، با اتهامات مشابهی مواجه شد.



گردآورنده: حسین علیمرادی

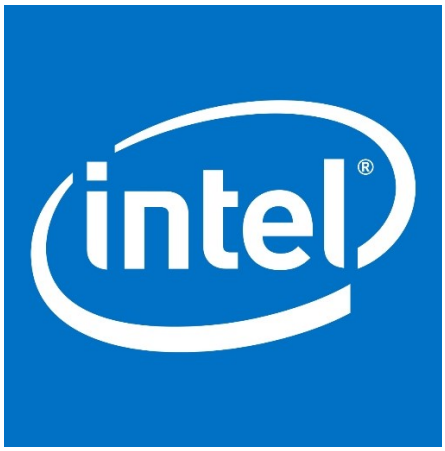
پیشنهاد جدید اینتل برای کمک به ایمن سازی خودکار دستگاه‌های اینترنت اشیاء

محصول جدید اینتل به نام Intel Secure Device Onboard (Intel SDO)، به عنوان یک سرویس به ارائه دهندگان پلت فرم‌های IoT ارائه خواهد شد تا در سریع-ترین زمان ممکن راهکاریی برای نصب بسته-های به روز رسانی و مدیریت هزاران دستگاه متصل را ارائه دهند. با اینتل SDO، شرکت می‌گوید، آوردن یک دستگاه به صورت آنلاین، تنها چند ثانیه طول می‌کشد.

طبق گفته اینتل، محصول جدید همچنین شیوه‌های امنیتی ضعیف مانند انتقال رمزهای عبور پیش فرض را حذف می‌کند و همچنین یک مدل حریم خصوصی برای IoT ارائه می‌دهد. Intel SDO همرا با شناسه ارتقا حریم خصوصی اینتل (Intel EPID)، راه حل حفظ حریم خصوصی IoT شرکت است که اجازه می‌دهد دستگاه‌ها به طور ناشناس تأیید شوند و یک تونل ارتباطی رمزگذاری شده را ایجاد می‌کند که مانع از دسترسی هکرها به دستگاه می‌شود.

EPID قبل از اینکه به یک دستگاه متصل شود، از اینتل SDO، هویت TCG / ISO و استاندارد احراز هویت را برای تایید رمزنگاری دستگاه مورد استفاده قرار می‌دهد اینتل EPID می‌تواند حریم شخصی خود را بوسیله حصول اطمینان از ورود دستگاه افزایش می‌دهد و به روز رسانی نرم افزار تهیه شده، ناشناس تر و امن تر خواهد بود.

یکی از مسائل اصلی، انتقال مالکیت است. به طور معمول، تولید کنندگانی که تعداد زیادی از دستگاه‌ها را تولید می‌کنند و به فروش می‌رسانند، نمی‌دانند که در چه محیطی



محصولات خود را به کار گیرند، که در هنگام تلاش برای حمایت از سفارشات مشتری باعث افزایش هزینه‌ها می‌شوند.

سرویس جدید اینتل، تقریبا سازگاری با تمام سیستم عامل‌های IOT را فراهم می-کند. برای اطمینان از در دسترس بودن گسترده، این شرکت با ارائه دهندگان سیلیکون مانند Infineon، Microchip و Cypress Semiconductor مشارکت کرده است تا قابلیت هویت EPID را در سخت افزارشان جاسازی کند. علاوه بر این، پلتفرم سرویس ابری و ارائه دهندگان نرم افزار مدیریت دستگاه مانند Google Cloud، Amazon Web Services (AWS)، Microsoft Azure و Intel's Wind River Helix Device Cloud نیز این ادغام را برای پشتیبانی از مدل zero touch اینتل SDO ارائه می-دهند. اینتل می‌گوید که تمام زنجیره ارزش را پوشش داده است: هویت اینتل EPID در سیلیکون جاسازی خواهد شد، تولید کنندگان نرم افزارهای مشتری را به کد بوت اضافه می‌کنند تا ارتباطات ناشناس را وارد کنند، صاحبان مجوز دریافت مالکیت دیجیتال خود را بارگذاری خواهند کرد، پلت فرم IoT از API برای فعال کردن ثبت دستگاه استفاده می‌کند و دستگاه در نهایت با Intel SDO تماس خواهد گرفت تا اثبات صحت آن را در اختیار شما قرار دهد.

این شرکت در توضیح محصول Intel SDO می‌نویسد "اینتل SDO به طور قابل توجهی به دستگاه‌های IoT قابل اعتماد onboard - از چند دقیقه تا چند ثانیه- شتاب می دهد همراه با zero touch، فرآیند خودکار زمانی که دستگاه برای اولین بار روشن می‌شود، آغاز می‌شود و زمانی که ارائه دهنده خدمات IoT انتخاب با یک زنجیره‌ی اعتماد خط مبنا از ارائه دهنده سیلیکون از طریق پلتفرم کنترل IoT کنترل می شود، پایان می‌یابد."

گردآورنده: حسین علیمرادی

یاهو: ۳ میلیارد حساب کاربری از سال ۲۰۱۳ در معرض خطر است

همانطور که همه‌ی ما از دیرباز شرکت یاهو را می‌شناسیم، این شرکت یکی از شرکت‌هایی است که بیشتر افراد برای رد و بدل کردن اطلاعات حساسشان از سرویس‌های مختلف آن استفاده می‌کنند. سرویس ایمیل یاهو یکی از سرویس‌هایی است که از دیر باز مورد توجه افراد قرار گرفته است و کاربران زیادی برای استفاده از این سرویس‌ها در یاهو اقدام به ایجاد حساب کاربری نموده‌اند.

نقص بزرگ اطلاعات حساب های کاربری یاهو در سال ۲۰۱۳، قبل از اینکه Verizon این شرکت را به دست آورد، باعث ایجاد آشفتگی بزرگی در آن شد، اما این آسیب ظاهرا هنوز به پایان نرسیده است. در ابتدا، به نظر می‌رسید ۱ میلیارد نفر از این نقض امنیتی تحت تاثیر قرار گرفته‌اند اما این تعداد همچنان افزایش می‌یابد. بیش از ۳ میلیارد نفر ممکن است تحت تاثیر این نقص قرار گیرند، این امر بزرگترین سرقت اطلاعات کاربران تا به امروز است.

یاهو نیازمند کاربرانی بود که به طور بالقوه تحت تاثیر هک قرار گرفتند تا رمزهای عبور خود را در سال ۲۰۱۶ تغییر دهند. اکنون اعتقاد بر این است که تمامی کاربران یاهو تحت تاثیر سرقت اطلاعات رمزگذاری شده در سال ۲۰۱۳ قرار گرفته اند. خوشبختانه هیچ داده‌ی شخصی از بین نرفته است، اما کلمات عبور ضعیف و افزایش قدرت محاسباتی می‌تواند به آسانی روش‌های امنیتی را از بین ببرد.

در زمان سرقت داده‌ها، یاهو از الگوریتم هش MD5 برای محافظت از کلمه عبور کاربری استفاده می‌کرد. از آن زمان، مشخص شد که MD5 از نظر رمزنگاری نا امن است و نباید برای سیستم‌های جدید استفاده گردد. یاهو بر اساس نقص امنیتی پیش آمده، استفاده از الگوریتم‌های رمز نگاری Bcrypt را که امن تر بوده و از salt (شامل بیت های تصادفی است که ورودی-های یک تابع یک طرفه را ایجاد می‌کند) های افزوده و مسیرهای چند گانه منطبق بر تابع هش بهره می‌بردند را جایگزین کرد.

اگر کاربر یاهو از سال ۲۰۱۳ بوده‌اید، هر گونه کلمه عبور و سوالات امنیتی که مورد استفاده قرار گرفته است برای استفاده در آینده نا امن می‌باشد. به یاد داشته باشید که پاسخ‌های پرسش امنیتی می‌تواند در واقع پاسخ به سوال پرسیده شده نباشد. هر عبارت می‌تواند به عنوان یک پاسخ امنیتی در نظر گرفته شود تا که زمانی که بتوانید آن را به یاد داشته باشید جهت کمک به حفظ امنیت حساب کاربری مفید خواهد بود.

گردآورنده: سمیه نیاخلیلی

چه اپلیکیشن‌هایی از اندروید و iOS اغلب توسط شرکت‌ها در لیست سیاه ثبت شده‌اند؟

براساس اطلاعات جمع آوری شده توسط Appthority، برنامه‌ها معمولا به دلیل این واقعیت که داده‌ها را از بین می‌برند؛ به لیست سیاه اضافه می‌شوند. رایج ترین برنامه‌ی iOS، whatsapp است که حاوی ریسک بالا با توجه به این واقعیت است که اطلاعات را از دفترچه آدرس دستگاه به یک سرور راه دور ارسال می‌کند. یکی دیگر از نرم افزارهای رایج در لیست سیاه، Pokemon Go است که به دفترچه تلفن و دوربین دسترسی پیدا می‌کند و مکان کاربر را دنبال می‌کند. Winzip هم چنین توسط بسیاری از سازمان‌ها ممنوع شده، به دلیل این که پیام های کوتاه ارسال می‌کند. این نوع رفتار می تواند خطر جدی در محیط سازمانی ایجاد کند. به ویژه اگر داده‌ها بدون رمزگذاری منتقل شوند.

بیشتر برنامه‌های iOS در لیست سیاه بالا در دسته بندی‌های شبکه‌های اجتماعی و سرگرمی قرار دارند؛ درمقایسه با اندروید که بسیاری از برنامه‌های لیست سیاه برنامه‌های کاربردی هستند. poot، یک ابزار است که به کاربران اجازه می‌دهد تا دستگاه‌های خود را روت کنند. برنامه‌های دیگر که معمولا ممنوع هستند عبارتند از: AndroidSystemTheme, Where's My Droid Pro, Weather, and Wild Crocodile Simulator.

در حالی که برخی از برنامه‌های اندروید، برای ردیابی محل کاربر یا ارسال داده بدون رمزگذاری، لیست سیاه شده است؛ در اغلب موارد ممکن است رفتار بدخواهانه را نشان دهد.

تجزیه و تحلیل ازبرنامه تلفن همراه iOS در محیط‌های سازمانی نشان داد که در مورد برنامه‌های اندروید، ۸۶/۷٪ از اتصالات به سرور واقع در ایالات متحده و سپس ایرلند با ۷/۷٪ ، آلمان ۲/۱٪ و سوئد با ۰/۷٪ است. در مورد اپ‌های iOS، نزدیک به ۹۴٪ از اتصالات به ایالات متحده آمریکا و سپس ایرلند با ۳/۸۲٪ و هلند و آلمان با سهم هرکدام ۰/۸۶٪ است.

گزارش Appthority نیز لیستی از ۱۰۰ برنامه برتر اندروید و iOS که در شرکت‌ها استفاده می‌شود همراه با نمره ریسک آن‌ها که می‌تواند به سازمان‌ها کمک کند تا خطرات مربوط به برنامه‌هایی که معمولا توسط کارکنان آن‌ها مورد استفاده قرار می گیرد را ارزیابی کند.

Domingo Guerra، رییس و یکی از بنیان گذاران Appthority توضیح داد:" تیم‌های شرکت‌های سازمانی باید درک کنند که کدام برنامه‌های تلفن همراه مورد استفاده قرار می‌گیرد. خطراتی که شاملشان می‌شود و همسالانشان از سیاست‌های تهدیدات تلفن همراه استفاده می‌کنند."

با BYOD و COPE، بسیاری از برنامه‌های کاربردی اندروید مورد تایید، راه خود را به شرکت‌ها می رسانند و خطراتی را برای داده-های حساس شرکت ایجاد می‌کنند.

۱۰ اپ تاپ iOS که وارد بلک لیست شده‌اند:

- Watssapp Messenger
- Pokemon Go
- Win zip
- Cam scanner
- Plex
- Wechat
- Facebook Messenger
- eBay Kleinanzigen
- Netease news
- Devise Alive

گردآورنده: حسین علیمرادی

یک ابزار تجزیه و تحلیل جدید از مایکروسافت برای مهندسان امنیت و توسعه دهندگان!

این ابزار که VulnScan نامیده می‌شود، توسط مرکز پاسخگویی امنیتی مایکروسافت (MSRC) طراحی و توسعه یافته است تا به تعیین نوع آسیب پذیری و علت اصلی نقص های فیزیکی حافظه کمک کند. این ابزار بر روی دو ابزار توسعه یافته داخلی، یعنی ابزارهای اشکال زدایی ویندوز (WinDbg) و اشکال زدایی زمان پیمایش (TTD) ساخته شده است. WinDbg به عنوان یک اشکال زدایی ویندوز ساخته شده است که به تازگی رابط کاربری طراحی را دریافت کرده است، در حالی که TTDیک چارچوب توسعه یافته داخلی است که برای ذخیره و اجرای برنامه های کاربردی ویندوز طراحی شده است. ماتوس کزویکی از MSRC توضیح می‌دهد "با استفاده از WinDbg و TTD، VulnScan قادر به ردیابی علت اصلی رایج ترین انواع مسائل مربوط به فساد حافظه است. مکانیزم تایید برنامه PageHeap نامیده می‌شود که برای رهاسازی یک نقض دسترسی نزدیک به علت اصلی مسئله مورد استفاده قرار می‌گیرد ".این ابزار فرآیند تجزیه و تحلیل را از محل تصادف آغاز می‌کند و سپس به منظور تعیین علت اصلی، پیشرفت می کند. VulnScan شامل پشتیبانی از پنج کلاس مختلف از مسائل مربوط به فساد حافظه، به نام‌های خارج از باند /read write، استفاده بعد از آزاد شدن (use after free) ،انواع سردرگمی، استفاده از حافظه‌ای که مقدار اولیه ندارد و حذف اشاره گر constant /NULL می‌باشد.

طبق گفته کزویکی، این ابزار همچنین می تواند سرریز و زیر ریز مربوط به عدد صحیح را همراه با دسترسی‌های خارج از باند ناشی از یک مقدار بد شمارنده حلقوی را تشخیص دهد. اشکالات مربوط به استفاده بعد از آزاد شدن، حتی بدون قابلیت PageHeap می تواند تشخیص داده شود. MSRC در حال حاضر از ابزار جدید به عنوان بخشی از چارچوب اتوماسیون خود به نام Sonar استفاده می‌کند که برای فرایند خارج از گزارش اثبات فایل‌های مفهوم طراحی شده است. این پلت فرم می‌تواند هر دو مسئله بازتولید و تجزیه و تحلیل علل ریشه‌ای را با استفاده از محیط‌های مختلف چند منظوره انجام دهد. مایکروسافت همچنین قصد دارد از VulnScan در سرویس تشخیص ریسک امنیتی مایکروسافت (Project Springfield) استفاده کند. به عنوان بخشی از این سرویس، آن را برای تصادم های de-duplicate و تجزیه و تحلیل گسترده آسیب پذیری‌های کشف شده توسط فازین مورد استفاده قرار می‌دهد. کزویکی می گوید: "طی یک دوره زمانی ۱۰ ماهه که VulnScan برای برطرف کردن همه مسائل مربوط به فساد حافظه برای Microsoft Edge، Microsoft Internet Explorer و محصولات Microsoft Office مورد استفاده قرار گرفت. این میزان موفقیت حدود ۸۵٪ بوده است، صرفه جویی در حدود ۵۰۰ ساعت زمان مهندسی برای مهندسان MSRC".

این ابزار از تجزیه و تحلیل ضعیف چندین شاخه‌ای استفاده می کند، به این معنی که می‌تواند به طور متوالی تمام مقادیر به دست آمده از یک دستورالعمل را ردیابی می‌کند. VulnScan همچنین یک صف از رجیسترها و آدرس‌های حافظه مربوط به موقعیت‌های خاص در جدول زمانی اجرای را نشان می دهد و تجزیه و تحلیل دقیق را به طور جداگانه برای هر شاخه انجام می‌دهد، به طوری که جریان داده‌های برنامه می‌تواند به طور کامل بازتولید شود.

گردآورنده: حسین علیمرادی

باج افزاری به نام RedBoot

یکی از خطرناکترین باج افزارهایی موجود که اخیرا کشف شده است RedBoot نام گرفته است. این باج افزار نه تنها فایل‌ها را رمزنگاری می‌کند، بلکه قادر به تغییر جدول پارتیشن و مستر بوت ریکورد (MBR) می‌باشد که به نظر می‌رسد این امر باعث آسیب دائمی خواهد گردید.

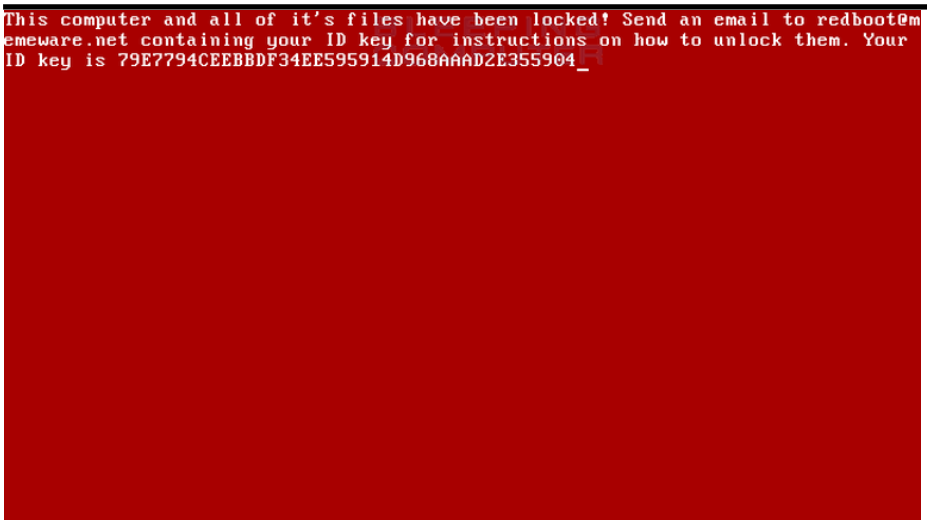
تحقیقات اولیه نشان می‌دهد که این باج افزار هیچ سرور کنترل و فرمانی ندارند و همچنین از قربانی هیچ درخواست باجی در واحد بیت کوین نمی‌گردد. با نتایج به دست آمده از این تحقیقات به نظر می‌رسد رمزنگاری غیر قابل بازگشت بوده و این باج افزار با هدف تخریب طراحی گردیده است.

البته این امکان وجود دارد که باج افزار RedBoot دارای ضعف در کد نویسی بوده باشد.

در حال حاضر هیچ نگرانی در خصوص آلوده شدن به این باج افزار وجود ندارد. توسعه دهندگان RedBoot در ارتباط با Abrams بیان نموده‌اند که این نسخه از باج افزار یک بیلد در حال توسعه می‌باشد. توسعه دهنده‌ی این باج افزار بیان نموده است که نسخه نهایی این باج افزار در ماه اکتبر در فضای مجازی پخش خواهد گردید. در این خصوص نیاز به احساس نگرانی می‌باشد.

باج افزار RedBoot چگونه کامپیوترها را تخریب می‌کند؟

نسخه‌ی فعلی باج افزار RedBoot به عنوان یک فایل اجرایی کامپایل شده از AutoIT



می‌باشد که دارای پنج بخش می‌باشد: یک اسمبلر، یک فایل boot.asm که اسمبلر آن را به boot.bin تبدیل می‌کند، یک فایل اجرایی که boot.bin را به یک MBR جدید تبدیل می‌کند، یک فایل اجرایی برای کدگذاری فایل‌ها و یک فایل اجرایی دیگر که از اجرای Task Manager جلوگیری می‌کند.

بعد از اینکه این باج افزار کار خودرا انجام داد کامپیوتر ریست می‌گردد و یک MBR جدید باعث بوت به یک صفحه‌ی قرمز رنگ می‌شود که شامل پیغامی است که کامپیوتر رمزنگاری گردیده است و باید برای رمزگشایی با توسعه دهنده ارتباط برقرار کرد.

همچنین این باج افزار جدول پارتیشن کامپیوتر را تغییر می‌دهد. چه کد نویسی این باج افزار ضعیف باشد یا خیر، این باج افزار بسیار خطرناک می‌باشد.

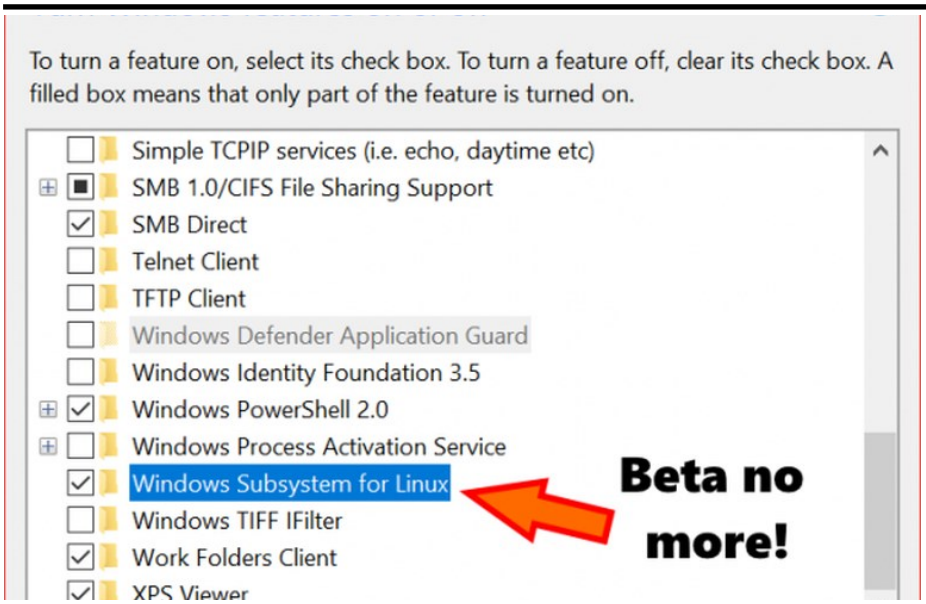
راه‌های حفاظتی پیشگیرانه

هیچ راهی وجود ندارد تا از ارتقاع این باج افزار تا ماه اکتبر بتوان آگاه شد و این مسئله با توجه به تمام آسیب‌هایی که این باج افزار می‌تواند به قربانی برساند بسیار نگران کننده است.

شرکت‌ها و افراد، نگران از دست رفتن فایل هایشان باید با ذخیره سازی فایل‌ها تحت شبکه و یا ذخیره سازی ابری اطمینان حاصل کنند، همچنین نرم افزارهای آنتی ویروس باید به روز رسانی شوند و کاربران برای جلوگیری از فیشینگ و سایر کلاهبرداری ها آموزش‌های لازم را ببینند.

گردآورنده: محمد مرتضوی

آغازی برای Bashware



محققان امنیتی Check Point می‌گویند که در Windows 10 Subsystem for Linux موسوم به WSL راهی برای اجازه دادن به بدافزارها برای نقض آنتی ویروس‌ها پیدا کرده‌اند.

WSL به فایل‌های باینری ELF لینوکس اجازه می‌دهد تا برروی ویندوز اجرا شوند. مایکروسافت این ویژگی را با هدف گسترش پشتیبانی خط فرمان ویندوز از ابزارها و همچنین کمک به توسعه دهندگان برای اجرای ترمینال Bash برروی ویندوز ۱۰ برای انجام امور مدیریتی معرفی نموده است.

این خصوصیت با در برگرفتن کامل ویژگی‌های مورد نیاز در آپدیت Fall Creators در ماه اکتبر در دسترس عموم قرار خواهد گرفت. استفاده از محیط WSL برای اجرای بدافزارهای لینوکس در محیط ویندوز و همچنین دور زدن تمامی راهکارهای امنیتی یکی از توانایی‌های این ویژگی است که محققان اصطلاح Bashware را برای توصیف آن معرفی نمودند. از آنجایی که ویژگی WSL تنها در ویندوز ۱۰ موجود می‌باشد، این آسیب می‌تواند برروی ۵۰۰ میلیون کامپیوتری که ویندوز ۱۰ سیستم عامل آنان است، تاثیر گذار باشد.

قابلیت‌های WSL به وسیله‌ی یک یک هسته شبیه ساز لینوکس و پردازش pico با اجرای فایل‌های باینری ELF برروی ویندوز امکان پذیر است. WSL همچنین قابلیت فراخوانی مستقیم هسته ویندوز را مهیا می‌کند. طبق گفته‌های Check Point، دو کلید sys. هسته لینوکس را شبیه سازی می‌کنند و فراخوانی‌های لینوکس را برای توابع API مربوط به ویندوز ترجمه می‌نمایند. طبق بیانات Check Point، یک Bashware با استفاده از شباهت بین قابلیت‌های فرآیندهای pico و پردازش‌های ویندوز NT، به یک مهاجم اجازه می‌دهد تا بدافزارهای ELF ویا EXE را به صورت مخفیانه اجرا نماید.

یک حمله تنها به چهار گام نیاز دارد. در ابتدا نیاز به فعالسازی WSL می‌باشد. سپس نیاز به فعالسازی حالت Developer Mode می‌باشد. تمرکز اصلی مایکروسافت برروی حملات در حالت User Mode می‌باشد. در هرحال، اگر یم مهاجم بتواند تمامی این گام‌ها را اجرا و به دست آورد، تنها کافیست که یک نمونه لینوکس را برروی ویندوز قربانی نصب کند.

هدف نهایی پژوهشگران در این پروژه این بود که ثابت کنند می‌توان از نرم افزارهای مخرب از سوی لینوکس به ویندوز حمله کنند. هرچند که هدف WSL انجام چنین اموری نمی‌باشد. Wine نیز به آن‌ها اجازه می‌دهد تا نرم افزارهای مخرب ویندوز را از طریق WSL اجرا کنند و این حملات را از دید محصولات امنیتی پوشش دهند.

همانطور که محققان بیان می‌کنند، Bashware با استفاده از وجود نقص در اجرای WSL بهره نمی‌رد، بلکه WSL یک ابزار جدید است که مرزهای شناخته شده ویندوز که اکثر محصولات امنیتی آنرا اسکن می‌کنند را گسترش می‌دهد.

با این حال شرکت‌ها باید ابزارهای امنیتی و فایروال‌های WSL را که مایکروسافت در دسترس قرار داده است به کار گیرند.

گردآورنده: محمد مرتضوی

۱۰ آسیب پذیری مهم در D-Link

پیر کیم، یکی از محققان امنیتی، تصمیم گرفت تا عموم آسیب پذیری‌های مربوط به روترهای D-Link 850L را در معرض عموم قرار دهد. برای افشای این مشکلات با شرکت‌های مربوطه هماهنگی های لازم به عمل آمده است. بنا به گفته‌ی محقق، نقص-های zero day، اگر توسط هکرها به کار گرفته شوند-، بالقوه می‌تواند منجر به دسترسی به root دستگاه‌ها و دسترسی از نوع Backdoor توسط مهاجمان گردد. هم چنین آن‌ها می‌توانند از راه دور اقدام به hijack و کنترل روترها کنند. هم چنین به کاربران آسیب پذیر حملات command injection، XSS و ... بزنند.

کیم قبلا آسیب پذیری‌هایی که برروی روترهای D-Link تأثیر می‌گذارد را گزارش کرده بود اما این شرکت از این آسیب پذیری-ها چشم پوشی کرد. این امر منجر به تصمیم محققان برای آشکارسازی نقص‌های zero day شد.کیم در یک بلاگ جزئیات این رخنه‌ها را منتشر کرده است. D-link 850L یک روتر است که به طور کلی با آسیب پذیری‌های زیادی طراحی شده است. اساسا، همه چیز از LAN تا WAN وخیم شده بود. حتی یک پروتکل کلود اختصاصی MyDlink مورد حمله قرار گرفته بود. عدم توجه آنها در مورد امنیت در گذشته، باعث شد تا بدون هماهنگی با آن‌ها این تحقیق را منتشر کنم". **این** محقق همچنین توصیه کرده کاربران فوراً روترهای آسیب پذیر را از اینترنت قطع کنند.

در اینجا فهرستی از ۱۰ آسیب پذیری zero day است که بر دو نسخه D-Link 850L A و B تأثیر می‌گذارد.

ضعف حفاظتی Firmware

عدم وجود حفاظت مناسب برای firmware می‌تواند به هکرها اجازه دهد تا یک firmware مخرب بر روی روتر آپلود کنند. گرچه firmware هایی که برای D-Link- مدل LRevB ۸۵۰ هستند یک هسته سخت محافظتی برای رمزها دارند، firmware مدل D-Link 850LRevA هیچ نوع محافظتی برای رمزها ندارد.

رخنه‌های Cross-site scripting (XSS)

کیم می‌گوید که شبکه LAN و WANمدل D-Link 850L RevA هر دو تحت تاثیر معایب several trivial XSS هستند که می‌تواند به هکرها این اجازه را بدهد تا کوکی-های احراز هویت را سرقت کنند.

رمز های عبور ادمین آسیب پذیرند

رخنه‌هایی که بر روی شبکه LAN و WAN مدل D-Link 850L RevB وجود دارد می‌تواند به مهاجمین این اجازه را بدهد تا گذرواژه‌های مدیریتی را بدست آورند و از پروتکل Cloud MyDLink برای دسترسی کلی به روتر قربانی استفاده کنند.

ادامه در صفحه بعد.

گردآورنده: محمد مرتضوی

۱۰ آسیب پذیری مهم در D-Link (ادامه...)

فقدان پروتکل مناسب برای Cloud

این نقص بر روی هر دو مدل D-Link 850L RevA و RevB تاثیر می‌گذارد. کیم متوجه شد که پروتکل MyDLink بدون رمزگذاری برای حفاظت از ارتباطات بین روتر و حساب کاربری MyDLink کاربران استفاده می‌کند.

دسترسی به Backdoor

روترهای D-Link 850L RevB دارای دسترسی درب پشتی از طریق Alphanetworks می‌باشند، و این امر به طور بالقوه به هکرها اجازه دسترسی root را می‌دهد.

Firmware همراه با کلید های خصوصی رمزگذاری می شود

این محقق همچنین کشف کرد که کلیدهای رمزگذاری خصوصی در فرم ور D-Link 850L RevA و RevB، می‌تواند به هکرها برای راه اندازی حملات MITM کمک کند.

عدم تأیید اعتبار

این مسئله می‌تواند هکرها را مجاز به تغییر تنظیمات DNS روترهای تحت تاثیر کرده و اساسا hijack را روی دستگاه را اجرا کنند.

پیش تایید اعتبار RCE ها به عنوان root

این مسئله روترها را برای حملات command injection، آسیب پذیر می‌کند، به طوری که به مهاجمان اجازه دسترسی root در دستگاه‌های تحت تاثیر را می‌دهد.

مجوزهای ذخیره شده در متن به طور واضح و ضعیق بودن مجوز فایل

در هر دو مدل D-Link 850L RevA و RevB مجوزها در متن به صورت واضح و فایل‌های محلی یافت می‌شوند.

باگ عدم دسترسی به سرویس (DoS)

این نقص می‌تواند به هکرها اجازه دهد تا از راه دور تجهیزات آسیب پذیر را خراب کنند.

کمیسیون تجارت فدرال ایالات متحده - FTC - اخیرا از D-Link شکایت کرده و ادعا کرده است که این شرکت تایوانی اقدامات امنیتی را به صورت ناقص انجام داده است که نتیجه آن باعث شده تا محصولات و کاربران به هک آسیب پذیر شوند. IBTimes انگلیس این مقاله را به دست D-Link رسانده است.

D-Link®

Building Networks for People

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