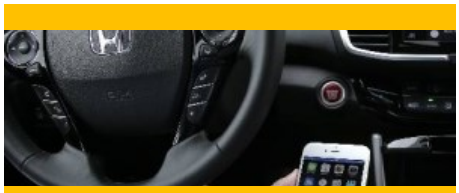
شماره دوم - اسفند ۱۳۹۵

خبرنامه "آپا" دانشگاه خوارزمی

در این شماره خواهید خواند:

هکر ها در قبال پاک نکـرد اطـلاعـات iDevice ها متقاضی باج از اپل شدند!

یک گروه از هکرها ادعا کردند کـه بـه ۳۰۰ میلیون حساب کاربری اپل دست پیدا کـرده اند. - صفحه ۲

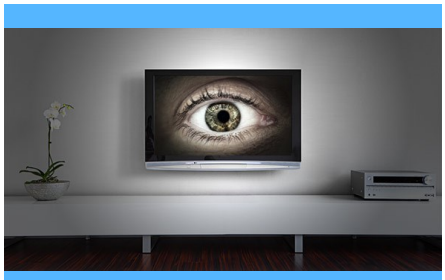


هشدار در خصوص خودروهای دست دوم

برخی از صاحبان قدیمی می توانند اتومبـیـل هایی که سالها قبل فروخته انـد را ردیـابـی کنند.- صفحه ۵

آسیب پذیری ناشناختـه جـدیـد در Apache Struts

محققان امنیتی یک آسیب پذیری ناشناختـه (Zero-Day) را در قالب اپلیکیشن محبوب تحت وب Apache Struts کشف کرده اند، که به صورت فعال در حال سوء استفاده شدن است. - صفحه ۸



جاسوس های تازه وارد!

در این هفته شرکت ویزیو کـه بـرنـدی بـا کیفیتی در تولید و ساخت تلویـزیـون مـی باشد، پذیرفت که مبلغ ۲.۲ میـلـیـون دلار جریمه، بخاطر جـاسـوسـی از خـریـداران بپردازد- صفحه ۳

بدافزارهای پیش از نصب اندرویدی

حداقل ۳۶ مدل از گوشی های هـوشـمـنـد متعلق به شرکت هـای مـحـبـوب مـثـل Samsung, LG, Xiaomi, Asus, Nexus, Oppo, Lenovo، که توسط دو شرکته ناشناس تـوزیـع مـی شـونـد، بـا بدافزارهای پیش از نصب یافت شـده انـد.- صفحه ۶ و ۷

تروجان Triada

پژوهشگران امنیت آواست دریافتند تروجان triada که سال گذشته به عنوان پیشرفته ترین تهدید موبایل شناخته شد، قابلیت های ضد تشخیصی خود را با انتخاب تکنولوژی سندباکس تقویت کرده است. صفحه ۴

دستگاه‌های IoT به شکل ناگهانی ردپای دیجیتالی شما را نشر می‌دهند!

دستگاه‌های IoT (دستگاه‌های دارای شبـکـه اینترنت داخلی) بشـدت مـورد عـلاقـه ی مصرف‌کنندگان و تجارت پـیـشـگـان اسـت. دستگاه‌های IoT نیز می‌تـوانـنـد خـطـرات بزرگی برای سازمانها ایجاد کنند، بوسیلـه ی نشر ناگهانی سطح حضور آنها. تـمـام ایـن وسایل، فرصتی برای ارتکاب جرایم سایبری را فراهم می‌کنند. - صفحه ۹

هکر ها در قبال پاک نکرد اطلاعات iDevice ها متقاضی باج از اپل شدند!

یک گروه از هکرها که خودشان را خانواده تبهکار ترکی می نماند ادعا کردند که به ۳۰۰ میلیون حساب کاربری اپل دست پیدا کرده اند. در صحبت با سایت "مادربورد"، هکر ها گفته اند که آنان در ارتباطی که با تیم امنیتی اپل داشته اند درخواست ۷۵۰۰۰ دلار پول در واحد بیت کوین و یا ۱۰۰۰۰۰ دلار کارت هدیه ی iTunes را دارند.

بنابر گزارشی، این تیم از هکرها تصاویری از صفحه مانیتور مبنی بر دسترسیشان بر اکانت ها به تیم امنیتی اپل ارائه نموده اند. هکرها همچنین یک فیلم از نحوهی چگونگی ورودشان به حساب های کاربری در یوتیوب به اشتراک گذاشته اند که گفته ها حاکی از آن است که حساب کاربری دزدیده شده در فیلم مربوط به یک خانم مسن می باشد.

اخبار حاکی از آن است که تیم امنیتی اپل از هکرها درخواست کرده تا فیلم مورد نظر از روی یوتیوب حذف گردد اما هکرها به این هشدار بی توجه بودهاند. این شرکت اعلام نموده است که از این تیم به هیچ عنوان از بابت نفوذشان تقدیر نخواهد شد و این عمل نه تنها دارای پاداش نمی باشد بلکه این اسناد و مدارک ارسالی به مقامات بلند پایه برای بررسی های بیشتر ارسال خواهد گردید.

آن گونه که از نشریات و اخبار مشخص است این تیم از هکرها اعلام نموده است که در صورت رد درخواستشان توسط اپل تا ۷ اپریل، تعدادی از حساب های کاربری iCloud را به تنظیمات اولیه برخواهند گرداند و با دسترسی از راه دور اطلاعات دستگاه های کاربران را پاک خواهند نمود.

به گفته ی سایت مادربورد در این ادعا چندین تناقض وجود دارد. در یک مورد آنان ادعا نمودند که ۵۵۹ میلیون حساب کاربری را مورد هدف قرار داده اند نه ۳۰۰ میلیون. همچنین استفاده از حساب های کاربری تقلبی و تصاویر ارسالی ساختگی نیز امر دشواری نبوده و ممکن است که این تیم در ارائه ی اسناد و شواهد به شرکت اپل مبالغه کرده باشند. البته احتمال دسترسی این تیم از هکرها به حاسب کاربری میلیون ها نفر از کاربران اپل نیز به هیچ عنوان تا کنون رد نشده است.

به احتمال زیاد برای جلوگیری از هرگونه مداخله ی غیر قانونی اپل تا ۷ اپریل راهی خواهد یافت. عوض کردن رمز عبور و فعالسازی احراز هویت دو مرحله ای تا ۷ اپریل می تواند راهکارهای پیشنهادی برای حفظ امنیت سایر کاربران باشد.

گردآورنده: محمد مرتضوی

iDevices

Innovations & Inventions for the future

تلویزیون های هوشمند؛ جاسوس های تازه وارد!

در این هفته شرکت ویزیو (Vizio) که برندی با کیفیت و مقرون به صرفه در تولید و ساخت تلویزیون می باشد، پذیرفت که مبلغ ۲.۲ میلیون دلار جریمه را به کمیسیون فدرال جهانی (FTC) بخاطر جاسوسی و ثبت برنامه هایی که خریداران آن نگاه می کنند در سرورهای این شرکت بپردازد. این اطلاعات ثبت شده در اختیار کمپانی های تبلیغاتی قرار می گرفته تا این شرکت های تبلیغاتی بتوانند به صورت هدفمندتر عمل نمایند.

این کار کمی شرم آور به نظر می رشد. این درحالی است که سایر بسترهای تلویزیون های هوشمند اطلاعات شما را در سطح آی پی بدون به توجه شما به مزایده نخواهند گذاشت. البته شرکت های نظیر ال جی نیز که از سیستم عامل webOS استفاده می کنند محتوای مورد تماشای هر فرد را به صورت خودکار تشخیص می دهند.

خبر خوب این است که راه حلی وجود دارد که می توان کمپانی ها را از محتوای مورد تماشای مشتریان به دور نگه داشت. این راه کمی ساده و پیش پا افتاده به نظر می رشد اما بسیار موثر است.

یکی از راه های پیش پا افتاده دور نگه داشتن تلویزیون از اینترنت برای ارسال و دریافت داده های مختلف به سرورهای تبلیغاتی در سراسر جهان می باشد. به طور صادقانه باید گفت که خریداران این تلویزیون ها باید این کار را انجام دهند.

شاید کلمه ی باهوش بخاطر همین اعمال در تلویزیون های هوشمند باشد. همچنین صفحه های pop-up ناخواسته نیز در این تلویزیون ها بسیار شایع می باشد که می توان با خاموش کردن wi-fi از دست تمامی این موارد راحت شد.

گردآورنده: محمد مرتضوی

تروجان Triada

پژوهشگران امنیت آواست دریافتند تروجان Triada که سال گذشته به عنوان پیشرفته ترین تهدید موبایل شناخته شد، اخیرا قابلیت های ضد تشخیصی خود را با انتخاب تکنولوژی سندباکس تقویت کرده است.

برای اولین بار در ماه مارس سال گذشته، تروجانی برای به دام انداختن برنامه های دستگاه های اندرویدی با استفاده از نفوذ به zigot، کشف شد. این تروجان با معماری ماژولار خود، اساسا برای تغییر مسیر تراکنشهای پیامکهای مالی طراحی شده است و از این طریق به خرید محتویات اضافی یا سرقت پول کاربر اقدام می کند.

به تازگی، تروجان Triada از سندباکس منبع باز DroidPlugin استفاده می کند تا به صورت پویا برنامه ای را بدون نصب، بارگذاری و اجرا می کند. با کمک این سندباکس، تروجان Triada پلاگین های APK مخرب را بارگذاری می کند.بنابراین، با این روش آنها را بدون نصب، روی دستگاه اندروید اجرا می کند.

به دلیل اینکه مولفه های مخرب آنها در برنامه ی میزبان ذخیره نمی شوند، تشخیص این تروجان برای آنتی ویروس ها زمان بر است. تروجان مذکور با کمک تکنیک های مهندسی اجتماعی پخش می شود مثلا افراد قربانی را برای دانلود این تروجان فریب می دهند.زمانی که این تروجان نصب شد، ایکون خودش را مخفی می کند و بدون هشدار به قربانی، شروع به سرقت اطلاعات شخصی می کند.

پژوهشگران آواست بیان کردند که، اگرچه اولین نسخه ی این تروجان از فریم ورک DroidPlugin استفاده نمی کرد، اما در ماه نوامبر ، نسخه ی جدیدی تولید شده که از آن استفاده کرده است.

در حدود همان زمانی که نوع جدید Triada پدید آمد، برنامه نویس این بد افزار به DroidPlugin یک باگ out-of-memory را اطلاع داد.

این تروجان چهره خودش را به عنوان Wandoujia تغییر می دهد. Wandoujia یک بازار اندرویدی چینی است.

به علاوه، مشاهده شده است که این تروجان همه‌ی پلاگین‌های apk مخرب را در دایرکتوری asset مخفی می کند.

محققان می گویند: هر یک از این پلاگین ها اعمال مخرب اختصاصی خود را دارند تا اطلاعات را از قربانی جمع آوری کنند، از جمله: ربودن فایل ،نظارت رادیویی و غیره. یکی از این پلاگین با یک سرور در ارتباط است. اینکه چه دستورات و چه فعالیت هایی باید انجام شود وظیفه این سرور است.این کارها توسط apk های دیگر انجام می شود.

همچنین آواست بیان می کند که برنامه نویسان تروجان نامبرده، پلاگین های مخرب را در یک برنامه جمع آوری نمی کنند اما در عوض، آنها استفاده از سندباکس DroidPlugin را برای بارگذاری و اجرا انتخاب کرده اند.آنها به طور مشخص این اقدام را برای عبور کردن از تشخیص آنتی ویروس ها انجام داده اند.

برنامه میزبان شامل اعمال مخرب نیست و آنتی ویروس ها برنامه میزبان را تشخیص نمی دهند و برنامه میزبان را به لیست خود اضافه نمی کنند.

تا کنون، تنها یکی دو مورد از تروجان ها مشاهده شده است که از سندباکس ها برای هدف های غیراخلاقی و زشت استفاده می کنند.اما نمونه های بیشتری هم ممکن است آشکار شود.

آواست نتیجه گیری می کند : اگر چه استفاده از سندباکس ها برای اجرای یک برنامه بدون نصب آن راحت است، اما تروجان ها همچنین میتوانند از سند باکسها به طور مخربی استفاده کنند.

گردآورنده: حسین علیمرادی

محققان درباره خطر احتمالی موجود در خودروهای دست دوم هشدار می دهند.

برخی از صاحبان قدیمی می توانند اتومبیل هایی که سالها قبل فروخته اند را ردیابی کنند.

فن آوری های داخل خودرو مدام در حال پیشرفته شدن هستند. هر چه که سیستم های خودرو هوشمندتر می شوند، احتمال ریسک امنیتی بالقوه نیز افزایش می یابد، مخصوصا در خودروهای دست دوم.

به همین دلیل پژوهشگر شرکت IBM، چارلز هندرسون، در کنفرانس امنیت RSA در سانفرانسیسکو، توضیح داد که چگونه از طریق اپلیکشن موبایل توانسته بود خودرو ائی را که سالها پیش فروخته بود کنترل کند. این اپلیکیشن شما را قادر می سازد برخی از کارها را انجام دهید برای مثال قفل ماشین را باز کنید، بوق بزنید و حتی مکان خودرو را مشخص نمایید.

هندرسون به شبکه سی .ان .ان .تک گفت: "اگرچه خودرو هوشمند است، اما نه آنقدر که بتواند مالک خود را تشخیص دهد. بنابراین، قادر نخواهد بود بفهمد که فروخته شده است. در داشبورد کنترل خودرو، امکانی وجود ندارد که به راننده اطلاع دهد شخص دیگری به کنترل ماشین دسترسی دارد."

مشکل این است که ریست کارخانه ای در مورد سیستم یک خودرو هوشمند، دسترسی کاربران قبلی را به طور کامل قطع نمی کند. تنها نمایندگی های مجاز اولیه، قادرند دسترسی افراد را به یک وسیله تشخیص داده و آن را به طور دستی حذف نمایند.

معمولا جواب روشنی که به مالکان داده می شود در مورد کنترل بیشتر خودرو است. همچنین به نمایندگی ها اجازه داده شده تا خودشان دسترسی های وسیله نقلیه خود را لغو کنند. البته این راهکار نیز خودش خطر آفرین است: شخصی با دسترسی آزاد به خودرو، می تواند دسترسی خود مالکان را نیز قطع کند.

با اضافه کردن برخی فرم ها از سیستم نمایندگی مالک می تواند این مشکل را حل کند، اما هندرسون می گوید شرکتهای خودروسازی در مورد عدم توانایی کاربرانشان در بکارگیری این گزینه نگران اند.

وی ادامه داد: توضیحی که داده شده در مورد نگرانی ما از خطای کاربران است، اما بهرحال یک "پین سیستم" یا "سیستم احراز هویت" جهت تنظیم مجدد، پیشنهاد من خواهد بود.

وی هشدار داد هر کسی که اقدام به خرید خودرو دست دوم می کند، همشه باید دستگاه را چک کند تا مطمئن شود چه کسانی به تنظیمات مدیریت وسیله دسترسی دارند. بنابراین هنگام استفاده از ماشینهای دست دوم، از نمایندگی ها در مورد اپلیکیشن های موجود در آن، اطمینان یابد که صاحبان قبلی هنوز در حال کنترل ماشین نیستند.

گردآورنده: حسین علیمرادی

مراقب باشید! بدافزارهای پیش از نصب اندرویدی در ۳۶ نوع گوشی هوشمند یافت شدند!

آیایک گوشی جدید اندرویدی خریداری کردید؟

حداقل ۳۶ مدل از گوشی های هوشمند متعلق به شرکت های محبوب مثل Samsung, LG, Xiaomi, Asus, Nexus, Oppo, Lenovo، که توسط دو شرکته ناشناس توزیع می شوند، با بدافزارهای پیش از نصب یافت شده اند.

این بدافزارها، بعد از عملیات اسکن بدافزار Check Pointروی اندروید، دستگاههایی که تعیین هویت شده اند را آلوده می کند.

دو نوع خانواده بدافزار در دستگاههای آلوده شناسایی شده اند: Loki و SLocker

بر اساس یافته های محققان چک پوینت منتشر شده در blog post، این اپلیکیشن های مخرب، در سیستم عامل عرضه شده توسط تولید کنندگان گوشی های هوشمند اضافه نشده است، بلکه بعدا جایی دیگر در امتداد زنجیره تولید و قبل از وارد شدن گوشی ها به دو شرکت از کارخانه های سازنده، نصب می شود.

در اولین بازدید، در فوریه ۲۰۱۶، تروجان لوکی، در سمت راست هسته سیستم عامل اندروید دستگاه تزریق شده تا امتیاز قدرتمند روت را بگیرد.

همچنین، این تروجان شامل ویژگی های جاسوسی مثل تهیه لیستی از تمام برنامه های نصب شده، تاریخچه مرورگر، لیست تماس ها، تاریخ تماس هاو داده های مکان یابی است.

در سوی دیگر SLocker، یک ransomwareبرای موبایل است که دستگاههای قربانیان را به منظور باج گرفتن قفل می کند و هنچنین، از طریق Tor برای پنهان سازی هویت اپراتورهای آن ارتباط برقرار می کند.

لیست گوشی های هوشمند محبوب آلوده شده با بدافزار:

- Galaxy Note 2
- LG G4
- Galaxy S7
- Galaxy S4
- Galaxy Note 4
- Galaxy Note 5
- Xiaomi Mi 4i
- Galaxy A5
- ZTE x500
- Galaxy Note 3
- Galaxy Note Edge
- Galaxy Tab S2
- Galaxy Tab 2
- Oppo N3
- Vivo X6 plus
- Nexus 5
- Nexus 5X
- Asus Zenfone 2
- LenovoS90
- OppoR7 plus
- Xiaomi Redmi
- Lenovo A850

ادامه در صفحه بعد...

مراقب باشید! بدافزارهای پیش از نصب اندرویدی در ۳۶ نوع گوشی هوشمند یافت شدند! (ادامه...)

بک دور بدافزار ها به اپراتورش اجازه دسترسی نامحدود به دستگاه های را آلوده می دهد از دانلود، نصب و فعال کردن اپلیکیشن های مخرب اندرویدی گرفته تا پاک کردن اطلاعات کاربر و حذف نرم افزارهای امنیتی و غیرفعال کردن اپلیکیشن های سیستم، حتی دسترسی به سیستم شماره گیری تلفن های حق بیمه!

این اتفاق، بر خطرناک بودن زنجیره ی تولید ناایمن تاکید می کند، و کارشناسان در مورد امنیت زنجیره تولید با بیش از ۲۰ مورد گزارش که در آن خرده فروشان حقه باز موفق به نصب نرم افزارهای مخرب بر روی گوشی های اندرویدی شده اند،ابراز نگرانی کرده اند.

نحوه حذف آلودگی های بدافزارها:

بعد از نصب بدافزارها بر ROM دستگاهها و استفاده از امتیازات سیستم عامل، خلاصی از آلودگی های آن بسیار دشوار است.

به منظور حذف بدافزار ها از دستگاه های آلوده، می توانید دستگاه خود را روت کنید و به راحتی بدافزار را از حالت نصب خارج نمایید. یا اینکه باید به طورکامل سیستم عامل و ROM گوشی خود را از طریق فلش کردن نصب مجدد کنید.

فلش کردن یک فرآیند پیچیده است،و توصیه می شود کاربران دستگاه خود را خاموش نموده و آن را به تکنیسین موبایل مورد تأیید نشان دهند.

این اولین بار نیست که گوشی های هوشمند با اپلیکیشن های مخرب مورد هدف قرار می گیرند.

در ماه دسامبر سال گذشته، گوشی های هوشمند و تبلت های اندرویدی ارزان قیمتی یافت شدند که حامل بدافزارهای مخرب بودند که این بدافزار ها، داده هایی در مورد دستگا ههای آلوده و نمایش تبلیغات در بالای اپلیکیشن های حال اجراء و دانلود APK های ناخواسته بر دستگاه های قربانی جمع آوری کرده بود.

در ماه نوامبر، محققان در AdUps سیستم عامل بیش از ۷۰۰ میلیون گوشی هوشمند اندرویدی یک بک دور مخفی کشف کردند که به صورت مخفیانه داده های صاحبان گوشی را جمع آوری کرده و به سرور چینی اش بدون اطلاع کاربر ارسال کرده است.

در همین حال، یک نقص در سیستم عامل Ragentek توسط برخی دستگاه های اندرویدی کم هزینه نیز کشف شد که به مهاجمان می دهد از راه دور کدهای مخرب را با دسترسی به روت و به دست گرفتن کنترل کامل دستگاه توسط هکرها اجراء کنند.

گردآورنده: حسین علیمرادی

آسیب پذیری ناشناخته جدید در Apache Struts

محققان امنیتی یک آسیب پذیری ناشناخته (Zero-Day) را در قالب اپلیکیشن محبوب تحت وب Apache Strutsکشف کرده اند، که به صورت فعال در حال سوء استفاده شدن است.

Apache Struts ک قالب منبع باز رایگان با معماری MVC برای ساخت اپلیکیشن های مدرن وب جاوا است که از ,REST AJAX, JSON پشتیبانی می کند.

در پست منتشر شده در روز دوشنبه، شرکت هوش سیسکو تالوس اعلام کرد که تیمش تعدادی از حملات فعال را در برابر آسیب پذیری zero-day (CVE-2017-5638) را در Apache Struts مشاهده کرده است.

به گفته محققان، این موضوع یک آسیب پذیری در اجرای کد از راه دور در تجزیه کننده مخرب جاکارتا متعلق به Apache Struts است که به مهاجمان اجازه می دهد تا دستورات مخرب را روی سرور در هنگام آپلود فایل ها بر اساس تجزیه کننده اجرا کنند.

آپاچی هشدار داد: ‘‘ممکن است یک حمله RCE از نوع محتوای مخرب انجام شود، اگر نوع محتوا معتبر نباشد، یک استثناء پس زده می شود که سپس برای نمایش پیام خطا به کاربر مورد استفاده قرار می گیرد.’’

این آسیب پذیری، مستند شده در قالب Rapid7's Metasploit Framework GitHub site، توسط آپاچی ترمیم شده است. بنابراین، اگر شما در حال استفاده از آپلود فایل بر پایه جاکارتا تحت Apache Struts 2 هستید، پیشنهاد می کنیم هر چه سریعتر Apache Struts نسخه ۲.۳.۳۲ یا ۲.۵.۱۰.۱ را ارتقاء دهید.

کد عمومی سوءاستفاده منتشر شد!

از همان زمان که محققان تالوس کد عمومی سوء استفاده (PoC) را شناسایی کردند (که توسط یک سایت چینی آپلود شده بود) ، این آسیب پذیری کاملا خطرناک است.

محققان حتی »شمار زیادی از سوء استفاده ها «را شناسایی کردند، که اکثریت آن به طور عمومی PoC منتشر شده ای است که برای اجرای دستورات متنوع مخرب استفاده می شود.

در برخی موارد، مهاجمان دستورات ساده "whoami"را اجراء می کنند تا ببینند که آیا سیستم هدف آسیب پذیر است یا خیر؛ در حالی که برخی موارد دیگر، حملات مخرب فرآیندهای فایروال را روی هدف خاموش کرده و داده انتقالی (payload) را کاهش می دهند.

محققان می گویند: »مراحل نهایی شامل دانلود کردن داده ی انتقالی مخرب از یک وب سرور، و اجرای آن است .«این داده ها متنوع اند اما شامل IRC bouncer و ربات DoS و یک نمونه مربوط به باتنت بیل گیتس می شوند ... یک داده انتقالی از یک حساب دارای امتیاز ویژه دانلود و اجراء شده است.

همچنین، مهاجمان تلاش کردند تا میزان مقاومت میزبان آلوده را با اضافه کردن یک فایل باینری به روال عادی بوت آپ به دست بیاورند.

بر اساس گفته محققان، مهاجمان تلاش کردند تا فایل را به یک دایرکتوری بی خطر کپی کنند و مطمئن شوند که ‘‘فایلهای قابل اجرا و سرویس فایروال هردو، هنگام بوت شدن سیستم غیرفعال خواهند شد.’’

محققان آپاچی و سیسکو، ادمین ها را تا آنجا که ممکن است، به ارتقاء سیستم هایشان به Apache Struts version 2.3.32 یا ۲.۵.۱۰.۱ تشویق می کنند. ادمین ها می توانند به یک Multipart parser متفاوت نیز سوئیچ کنند.

گردآورنده: حسین علیمرادی

دستگاه‌های IoT به شکل ناگهانی ردپای دیجیتالی شما را نشر می‌دهند!

دستگاه‌های IoT(دستگاه‌های دارای شبکه اینترنت داخلی) بشدت مورد علاقه ی مصرف‌کنندگان و تجارت پیشگان است. همچنان که تجارت بی‌عیب و نقص همیشه برپایه‌ی داده بوده است، مصرف کنندگان نیز با داده و قابلیتهای کنترل از راه دور سازگار شده‌اند. کار با دستگاه‌های IoT راحت است و به ما امکان دسترسی به چیزهایی را میدهد که قبلا ممکن نبوده مگر اینکه شما بصورت فیزیکی در مقابل دستگاه می بودید. آنها همچنین برای ما داده‌های پرکاربردی برای انجام کارها و بهتر تصمیم گرفتن، تولید می‌کنند.

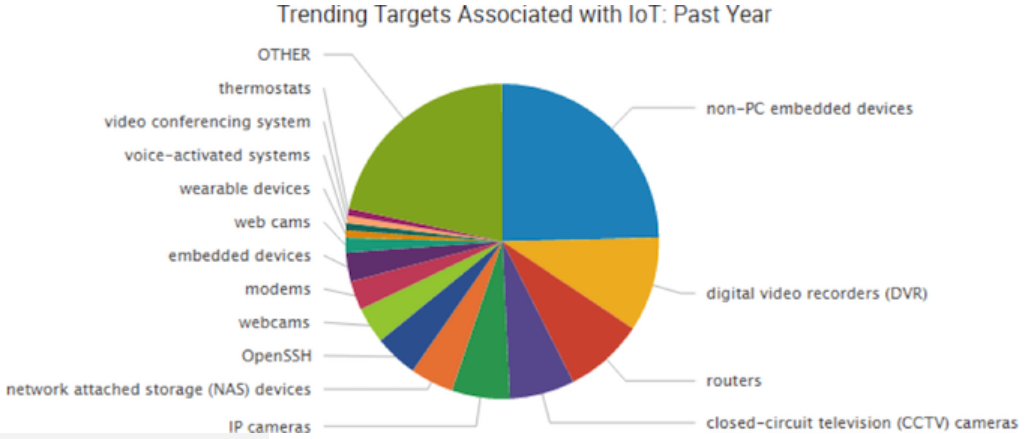
دستگاه‌های IoT به من حس تکرار لحظه ای از گذشته در زمان حال را میدهد... وقتی میگوییم من این را قبلا تجربه کرده‌ام، بارها...

در حدود سالهای ۲۰۰۰ تا ۲۰۰۵ هنگامی که ماشینهای مجازی کم کم تبدیل به تکنولوژی عصر "رفتن" شد، بسیاری از ماموران اطلاعاتی، بوسیله ی یکی کردن سخت افزار فیزیکی با محیط مجازی و ادعای صرفه‌جویی در هزینه ها، مشت خود را به نشانه ی موفقیت بالا بردند. فقط صرفه جویی در هزینه چیزی کم اهمیت میشود وقتی شما عامل توسعه‌ی زیاد ردپای دیجیتال میشوید، پیزی که در این دوره باید مواظبش بود و مدیریتش کرد.

با حرکت سریع تا سال ۲۰۰۹، یک کلمه ی جادویی بنام BYOD دستگاه شخصی خود را بیاورید) شروع به نمایش کرد. در حال حاضر ما داریم داده هایی را به وضوح باهم ترکیب میکینیم که نیاز به حفاظت بوسیله ی دستگاه‌های شخصی دارد. آیا تابحال مجبور به کشف مجازی یک وسیله ی BYOD شده اید؟ تجربه ی جالبیست. وقتی که گرایش به BYOD همه‌گیر شده بود، من یک مامور امنیت اطلاعاتی بودم و به جای اینکه برای اول بودن در آن عجله کنم، صبر کردم و روش را دیدم. تعداد داستانهای ترسناکی را که از مشکلات سازگاری با BYOD اولیه شنیده ام، قابل شمارش نیست.

درست شبیه ملزومات ماشین مجازی و BYOD همراه، دستگاه های IoT نیز میتوانند خطرات بزرگی برای سازمانها ایجاد کنند، بوسیله ی نشر ناگهانی سطح حضور آنها. تمام این وسایل، فرصتی برای ارتکاب جرایم سایبری را فراهم میکنند. من گزارشهای زیادی حاکی از افزایش تعداد دستگاه‌های "هوشمند" به دو یا سه برابر در ۴ سال آینده خوانده‌ام. بسیاری از این دستگاه‌ها مبتنی بر مصرف کننده هستند و فاقد ابزارهای امنیت سایبری پایه، و تحت مدیریت مرکزی نیز نیستند. فقط نگاهی به اداره ی خود بیاندازید و چه میبینید؟

در این نمودار زیر، تیم جاسوسی تحلیلی تهدیدی من در ازمایشگاه های سرف واچ، نگاهی به داده‌های تهدیدکننده طی سال گذشته و تمام دستگاه‌های IoT مورد هدفِ جمع شده، انداخته‌اند تا این خطر را پررنگ تر کنند. نیاز به گفتن نیست که راههای فراوان جدیدی برای ارتکاب جرایم سایبری از طریق پیدا کردن دسترسی ناشناخته به سیستم‌ها و اطلاعات مهم، وجود دارد.



گردآورنده: حسین علیمرادی

Kharazmi CERT Coordinator Center

مرکز آپا دانشگاه خوارزمی

مدیر مسئول:

دکتر امید مهدی عبادتی

هیات علمی:

دکتر احسان ملکیان

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)

وب سایت:

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