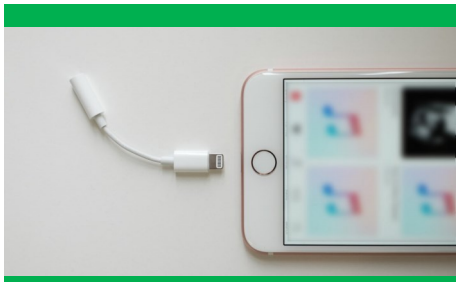
شماره هجدهم - تیر ۱۳۹۷

خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:



شرکت اپل وضعیت محدود جدید USB، که در مقابل ابزارهای کرک پلیس مقابله می‌کند را درگوشی iPhone تایید می‌کند

چه اتفاقی افتاده است؟ بنظر می‌رسد بین اپل و اجرای قانون نزاع رخ می‌دهد. شرکت کوپرتینوحضور سیستم عامل‌های iOS11.4.1، iOS12 را با یک خاصیت که حالت محدود USB نامیده می‌شود، را تایید

هکرها با استفاده از دستگاه کنترل از راه دور ۶۰۰ گالن سوخت را از ایستگاه گازی به سرقت می‌برند.

با روند رو به رشد قیمت گاز، به ازای ۳ دلار در هر گالن در ایالات متحده، بعضی از افراد به دنبال احیای زندگی و سود در پمپ‌های گاز هستند. اینکه هکرها چگونه با وجود مشکلات به کار خود ادامه می‌دهند، شاید بیشتر دسیسه یا فریب باشد تا اینکه دلیلی برای آن داشته باشند. - صفحه ۳

رفع آسیب‌پذیری‌های SmartThings Hub

با روند رو به رشد قیمت گاز، به ازای ۳ دلار در هر گالن در ایالات متحده، بعضی از افراد به دنبال احیای زندگی و سود در پمپ‌های گاز هستند. اینکه هکرها چگونه با وجود مشکلات به کار خود ادامه می‌دهند، شاید بیشتر دسیسه یا فریب باشد تا اینکه دلیلی برای آن داشته باشند. - صفحه ۴

هکرها با سو استفاده از روترهای MikroTik به استخراج ارز دیجیتال Monero پرداختند!

طی گزارشی بیش از ۱۷۰۰۰۰ روتر میکروتیک توسط هکرها برای استخراج ارز دیجیتال Monero مورد سو استفاده قرار گرفته‌اند. - صفحه ۵

گوگل: از زمانی که کاربران کلیدهای امنیتی را استفاده می‌کنند هیچ یک از آنان مورد حمله فیشینگ قرار نگرفته‌اند.

همانطورکه می‌دانیم تایید هویت چند مرحله‌ای، بهترین شیوه برای در امان ماندن از حملات فیشینگ می‌باشد که موثرترین روش آن استفاده از کلیدهای امنیتی است. - صفحه ۶

اسکیمرها

اسکیمرها اساسا کارت خوان های مخربی هستند که اطلاعات مربوط به نوار مغناطیسی کارت که به پایانه های پرداخت واقعی متصل می شوند را می گیرند تا بتوانند اطلاعات همه افرادی که کارتهایشان مورد سرقت واقع شده است را برداشت کنند. - صفحه ۷

شرکت اپل وضعیت محدود جدید USB، که در مقابل ابزارهای کرک پلیس مقابله می‌کند را درگوشی iPhone تایید می‌کند

چه اتفاقی افتاده است؟ بنظر می‌رسد بین اپل و اجرای قانون نزاع رخ می‌دهد. شرکت کوپرتینوحضور سیستم عامل‌های iOS11.4.1، iOS12 را با یک خاصیت که حالت محدود USB نامیده می‌شود، را تایید کرده است. این خاصیت ارتباط داده‌ای از طریق پورت لایتنینگ را در زمانی که به مدت یک ساعت قفل گوشی باز نشده است، غیرفعال می‌سازد.

با اتصال آن، مد متناهی بصورت پیش فرض فعال می‌گردد و تا زمانی که فعال است شارژ تنها عملکرد از طریق پورت لایتنینگ iPhone تا یک ساعت پس از قفل گوشی خواهد بود.

این خاصیت بدان معنی است که پلیس و دیگر مسئولین اجرایی تنها مدت زمان خیلی کوتاهی برای گسترش ابزارهای کرک iPhone از طریق شرکت‌های امنیتی شبیه GrayShift و Cellebrite و... را خواهند داشت. GrayKey بخصوص یک ابزار متداول و عمومی از GrayShift است که حداقل در ۵ ایالت و ۵ آژانس فدرال استفاده می‌گردد.

GrayKey از پورت لایتنینگ برای دسترسی به وسیله استفاده می‌کند و تلاش برای کرک پسوردها را بیش از حد معمول که اجازه داده می‌شود ممکن می‌سازد و وابسته به طول پسورد در هر جایی می‌تواند بین ۲ ساعت تا سه روز بطول بیانجامد.

اپل در گفتگو با رویترز بیان داشته است که قصد دارد از تمامی مشتریان خود خصوصا در کشورهایی که تلفن‌ها به آسانی و با منابع گسترده در دست نیروی پلیس و مجرمین قرار می‌گیرند، حفاظت کند و از گسترش بیشتر روش‌های حمله جلوگیری کند.

مُد محدود USB اخیرا در توسعه‌دهنده بتا برای هر دو سیستم عامل iOS11.4.1 و iOS12 قرار گرفته است. فایل ضمیمه (Patch) مربوطه نیز برای انتشار در آخرین نسخه iOS تنظیم شده است.

یک گزارش New York Times نشان می‌دهد که پلیس از طرح اپل رضایت ندارد اما شرکت اپل بر این موضوع اصرار دارد که این خاصیت به نفع مشتریان است و راهی برای محافظت از مجرمین نیست.

یک نماینده اپل بیان داشته است که: "ما دائما در حال تقویت محافظت‌های امنیتی در هر یک از محصولات اپل هستیم تا به حمایت مشتریان در مقابل هکرها، دزدان هویت و نفوذ به اطلاعات شخصی کمک نماییم. ما بیشترین احترام را برای اجرای قانون قائل هستیم و پیشرفت‌های امنیتی را به منظور تخریب تلاش آن‌ها برای انجام وظایفشان، طراحی نمی‌کنیم".

انتظار داشته باشید که این موضوع، مناقشه دیگری را در حوزه امنیت و حریم خصوصی ایجاد نماید؛ شبیه آنچه که بدنبال ماجرای آیفون سان برنادینو بوجود آمد. در سال ۲۰۱۶، شرکت اپل از کمک به اداره تحقیقات فدرال جهت باز نمودن قفل گوشی (iPhone c5) سید رضوان فاروق –یکی از تیراندازان سان برنادینو - امتناع کرد. مقامات فدرال نهایتا به یک شخص ثالث (Third Party) –تصور می‌شود Cellebrite باشد - روی آوردند.

گردآورنده: فاطمه الهی

هکرها با استفاده از دستگاه کنترل از راه دور ۶۰۰ گالن سوخت را از ایستگاه گازی به سرقت می‌برند.

با روند رو به رشد قیمت گاز، به ازای ۳ دلار در هر گالن در ایالات متحده، بعضی از افراد به دنبال احیای زندگی و سود در پمپ‌های گاز هستند. اینکه هکرها چگونه با وجود مشکلات به کار خود ادامه می‌دهند، شاید بیشتر دسیسه یا فریب باشد تا اینکه دلیلی برای آن داشته باشند.

پلیس دترویت به دنبال دو نفر است که گفته می‌شود یک پمپ گاز محلی را هک کرده‌اند تا صدها گالن سوخت را در روز روشن به سرقت برسانند.

سرقت در حدود ساعت ۱ صبح در ۲۳ ژوئن در ایستگاه خدمات ماراتن در دترویت، میشیگان رخ داده است. بر اساس گزارشات Fox2Detroit، پلیس اعلام کرد که دزدها از دستگاه کنترل از راه دور برای هک کردن پمپ استفاده می‌کردند که همچنین قادر بود تا مانع از کنترل کار پمپ در ایستگاه توسط منشی شود.

رسانه‌های محلی NEWS ۴ گزارش داده‌اند دوربین‌های نظارتی که در حال تماشا (ضبط فیلم) پمپ‌ها بودند در زمانی که دزدی رخ داد شکسته شدند. در هر حال دوربین‌های داخل ایستگاه از دو مظنون عکس گرفتند.

پلیس می‌گوید در طی حدودا ۹۰ دقیقه، ۶۰۰ گالن سوخت دزدیده شده است. گفته می‌شود که بیش از ۱۰ وسیله نقلیه – اما کمتر از ۲۰- برای حمل سوخت استفاده شده است.

پلیس نمی‌داند که آیا دزدان این سرقت را با همدستان خود برنامه‌ریزی کرده‌اند یا بسادگی نرخ تخفیفی را برای مشتریان ایستگاه شارژ کرده‌اند تا سوخت وسایل خود را در پمپ‌های هک شده تکمیل نمایند.

با حدود قیمت ۳ دلار در هر گالن، نتیجه می‌گیریم تقریبا ۱۸۰۰ دلار سوخت دزدیده شده است.

طبق گفته منشی ایستگاه Fox2Deetroit او سعی داشته است که پمپ را بصورت (نرم افزاری) خاموش کند اما ممکن نبوده است. وی تنها توانسته که پمپ را بصورت (سخت افزاری) با کلید خاموش کند و بعد از دریافت کیت اضطراری با پلیس تماس گرفته است.

گردآورنده: فاطمه الهی

رفع آسیب‌پذیری‌های SmartThings Hub

با روند رو به رشد قیمت گاز، به ازای ۳ دلار در هر گالن در ایالات متحده، بعضی از افراد به دنبال احیای زندگی و سود در پمپ‌های گاز هستند. اینکه هکرها چگونه با وجود مشکلات به کار خود ادامه می‌دهند، شاید بیشتر دسیسه یا فریب باشد تا اینکه دلیلی برای آن داشته باشند.

سامسونگ برای آسیب‌پذیری‌های اخیر SmartThings Hub که می‌توانند برای اجرای کدهای دلخواه در دستگاه‌های آسیب‌پذیر مورد استفاده قرار گیرند اصلاحیه ای منتشر کرد

SmartThings Hub که به‌عنوان یک کنترل‌کننده مرکزی طراحی‌شده است، به کاربران امکان نظارت و مدیریت دستگاه‌های هوشمند خانگی مانند پریزهای هوشمند، لامپ‌های LED، ترموستات، دوربین‌ها و ... را می‌دهد .کنترل‌کننده یک نرم‌افزار دائمی مبتنی بر لینوکس را اجرا می‌کند که امکان برقراری ارتباط با دستگاه‌های اینترنت اشیاء را فراهم می‌نماید که این دستگاه‌ها در استفاده خانگی از Ethernet، Zigbee، Z-Wave and Bluetooth به کار می‌روند.

مهاجم با استفاده ازآسیب‌پذیری‌های کشف‌شده، می‌تواند به اطلاعات حساس جمع‌آوری‌شده توسط هاب و دستگاه‌های متصل به هاب دسترسی پیدا کند و فعالیت‌های غیرمجازی انجام دهد مانند باز کردن قفل درب خانه -نظارت از طریق دوربین‌ها و یا غیرفعال کردن حسگرهای حرکتی .

درمجموع ۲۰ آسیب‌پذیری که بر SmartThings Hub تأثیر می‌گذارد، توسط محققان Talos کشف شد .این محققین این مطلب را فاش کردند که مهاجم می‌تواند سه کلاس آسیب‌پذیری که در دستگاه وجود دارد را باهم ادغام کند تا کنترل کامل دستگاه را در دست بگیرد .«همچنین در این پست وبلاگی، محققان خط سیرهای مختلف حمله را به‌مثابه یک عملگر توصیف می‌کنند که به دنبال بهره‌گیری این زنجیره‌های آسیب‌پذیری است که می‌تواند از آن‌ها استفاده کند.

آسیب‌پذیری‌ها در نسخه ۰.۲۰.۱۷ نرم افزار SmartThings Hub STH-ETH-250 سامسونگ -یافت شدند .سامسونگ تاکنون اصلاحاتی را برای همه نقص‌ها منتشر کرده و به کاربران توصیه می‌شود که دستگاه‌های خود را به‌روز نگه‌دارند تا امنیت را حفظ کنند (چراکه سامسونگ به‌روزرسانی را به‌صورت خودکار انجام می‌دهد و تعامل کاربر لازم نخواهد بود).

گردآورنده: حسین علیمرادی

هکرها با سو استفاده از روترهای MikroTik به استخراج ارز دیجیتال Monero پرداختند!

طی گزارشی بیش از ۱۷۰۰۰۰ روتر میکروتیک توسط هکرها برای استخراج ارز دیجیتال Monero مورد سو استفاده قرار گرفته‌اند. در پایان ماه جولای، محقق امنیتی Trustwave آقای Simon Kenin اشاره نمود که متوجه رشد شدید استفاده از نرم افزار Coinhive شده است که این نرم افزار امکان استخراج ارز دیجیتال Monero را توسط روترهای ساخته شده توسط شرکت MikroTik را به کاربر می‌دهد.

Simon Kenin دریافت که تمامی itreratrion ها در Coinhive از یک کلید استفاده می‌کنند. این امر بدین معنی است که تمامی ارزهای استخراج شده به یک اکانت فرستاده می‌شود. بر اساس تحقیقات این محقق، هکرها با استفاده از یک آسیب پذیری روز صفر در عنصر Winbox در روترهای MikroTik که در ماه آپریل کشف گردید، اقدام به این کار می‌کنند. MikroTik برای این آسیب پذیری در کمتر از یک روز، یک وصله نرم افزاری ارائه نمود اما این بدین معنی نیست که صاحبان روترها این وصله نرم افزاری را نصب کرده‌اند. این محقق امنیتی بیان می‌کند که در حدود صدها هزار روتر آسیب پذیر همچنان موجود است که بیشتر آنان در برزیل مستقر هستند.

Kenin بیان نمود : "من باید تاکید کنم که این حمله بد است، منظورم خیلی بد است. میلیون ها دستگاه در سراسر جهان وجود دارد که توسط این روترها خدمت رسانی می‌شوند. مهاجمان از این روش به جای حمله‌ی باج افزاری استفاده کرده‌اند. زیرا آنان درآمد بیشتری را به نسبت پرداخت باج توسط قربانی دریافت خواهند کرد. مهاجمان با ساتفاده از این حمله می‌توانند به صورت پیوسته درآمد داشته باشند. هدف آنان رسیدن به درآمدی بالاتر از درآند حاصل از حملات باج افزاری است."

Troy Mursch محقق امنیتی Independentحملات این چنینی را در کشور مولداوی مشاهده کرده است که برروی چیزی در حدود ۲۵۰۰۰ روتر MikroTik اسکریپت CoinHive نصب می‌باشد. Mursch در گذشته بیان کرده بود که: "به نظر من CoinHive یک ایده‌ی بسیار جالب می‌باشد. این اسکریپت قرار بود یک روش درآمدزایی برای وب سایت‌ها باشد. اما اکنون می‌بینیم که از این اسکریپت سو استفاده می‌شود و از آن به عنوان بدافزار استفاده می‌شود."

حتی CoinHive اعتراف کرد که برنامه آن‌ها به یک نیروی مخرب تبدیل شده است. CoinHive به روزنامه Suddeutsche Zeitung گفت: "ما نمیتوانیم نظر کاربر را انکار کنیم که نسل کاملا جدیدی از نرم افزارهای مخرب را اختراع کردیم. ما به آن افتخار نمی کنیم."

گردآورنده: محمد مرتضوی

گوگل: از زمانی که کاربران کلیدهای امنیتی را استفاده می‌کنند هیچ یک از آنان مورد حمله فیشینگ قرار نگرفته‌اند.

همانطورکه می‌دانیم تایید هویت چند مرحله-ای، بهترین شیوه برای در امان ماندن از حملات فیشینگ می‌باشد که موثرترین روش آن استفاده از کلیدهای امنیتی است.

فقط با پرسش از گوگل مشخص شده، با توجه به اینکه از اوایل سال ۲۰۱۷ نیاز بوده است همه کارمندان از کلیدهای USB استفاده کنند بطور موفقیت‌آمیزی حساب کاربری هیچ یک از کارمندان -بیش از ۸۵ هزار نفر-، مورد حمله فیشینگ قرار نگرفته است.

غول فن‌آوری در زمینه امنیت به کربز اظهار داشته است که: از زمان اجرای کلیدهای امنیتی در گوگل هیچ اعمال کنترلی بر روی حساب های کاربری، تایید یا گزارش نشده است.

ممکن است از کاربران خواسته شود تا با استفاده از کلیدهای امنیتی در برنامه ها یا به دلایل مختلف تایید هویت کنند. همه این‌ها به حساسیت برنامه و ریسک کاربر در آن نقطه از زمان بستگی دارد .

کلیدهای امنیتی جایگزین روش‌های معمول دو مرحله ای تایید هویتی شده‌اند که متکی بر ارسال یک پیام کوتاه و شامل یک کد می‌باشد.

در دستگاه های USB احتیاج است برای ورود کاربر به حساب خود کلید را وارد کنند و دکمه مربوطه را فشار دهند.

کلیدهای امنیتی نسبت به سایر روش های تایید هویت دو مرحله ای که در انها هکرها می‌توانند پیام‌های فرستاده شده به یک دستگاه را از طریق شیوه‌هایی چون جعل سیم کارت قطع نمایند، امن تر بنظر می-رسند.

هر کسی که سهوا اطلاعات هویتی خود را از طریق ایمیل‌های فیشینگ فاش نماید، به حساب کاربری وی تا زمانیکه کلید امنیتی در دست نفوذگران بداندیش قرار نگیرد مورد حمله واقع نمی‌شود. تنها نگرانی واقعی درباره از دست دادن امنیت زمانی بوجود می‌آید که کلید مفقود گردد.

گردآورنده: فاطمه الهی

اسکیمرها

اسکیمرها اساسا کارت خوان های مخربی هستند که اطلاعات مربوط به نوار مغناطیسی کارت که به پایانه های پرداخت واقعی متصل می شوند را می گیرند تا بتوانند اطلاعات همه افرادی که کارتهایشان مورد سرقت واقع شده است را برداشت کنند .

اسکیمرها ، دستگاه های تقلبی هستند که برای قرار گرفتن در بالای شکاف پذیرش دستگاه نقدی ساخته شده اند و معمولا با چسب یا نوار دو طرفه به دستگاه خودپرداز وصل می شوند .

اسکیمر ها ورودی اطلاعات کارت پرداخت را از نوار مغناطیسی در پشت کارت های وارد شده به دستگاه های هک شده ضبط می کند ، در حالی که یک دوربین جاسوسی پنهان بالا یا کنار صفحه کلید وجود دارد که یک ویدیو از دارنده ی کارت حین وارد کردن پین کد ضبط می کند .

این داده ها به سارقین اجازه می دهد تا کارت های جدید بسازند و از پین کد ها برای برداشت پول نقد از حساب قربانی استفاده کنند . مخفی کردن پین کد در حین تایپ به وسیله ی دست ، هر دوربین مخفی را از ضبط و نشان دادن پین کد شما منع میکند . این دوربین های مخفی در اکثریت قریب به اتفاق از بیش از سه جفت سیستم ردیابی ATM استفاده می کنند .

برای اطلاع از دستکاری شدن خودپرداز چک کنید

وقتی به یک دستگاه خودپرداز رسیدید ، قسمت بالای دستگاه خودپرداز ، نزدیک بلندگوها ، کنار صفحه نمایش ، خود کارت خوان (قسمتی که کارت را وارد می کنید) و صفحه کلید را برای برخی علایم واضح دستکاری شدن چک کنید .

اگر به چیز متفاوتی مثل رنگ و مواد مختلف ، گرافیک هایی که به درستی تنظیم نشده اند یا هرچیز دیگری که به نظرتان درست نیست ، برخورد کردید ، از آن دستگاه استفاده نکنید . همین امر برای دستگاه هایی که کارت های اعتباری را میخوانند هم صادق است .

چند راهکار وجود دارد که هرکسی باید با رعایت آنها موفقیت سارقین را به حداقل برساند .

به هگام وارد کردن پین ، از افشای آن جلوگیری کنید .

حدالامکان سعی کنید از استفاده از دستگاه های مستقل در مناطق کم نور پرهیز کنید .

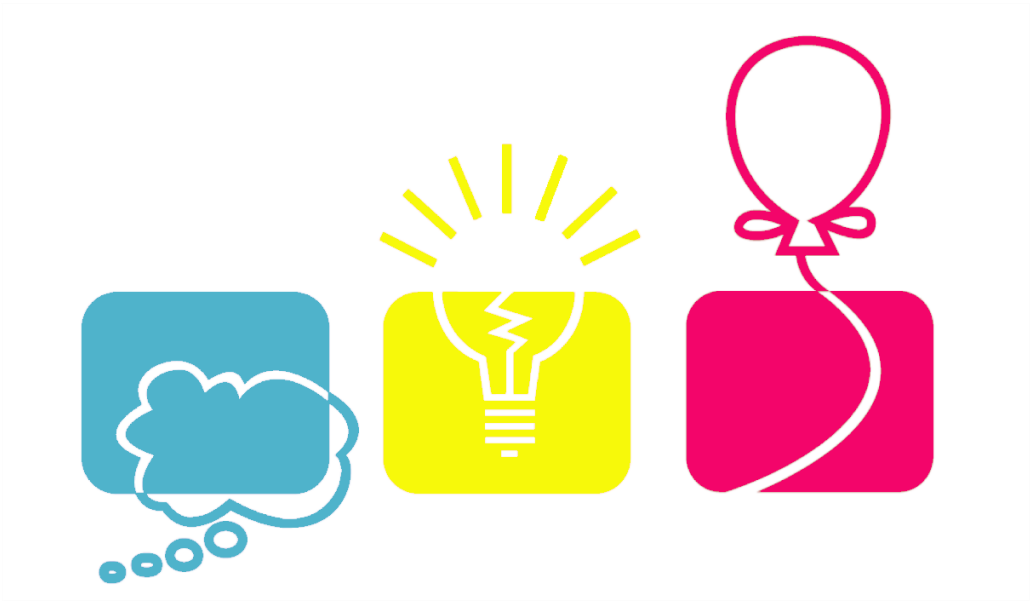
از دستگاه های خودپردازی که در بانک ها نصب شده اند استفاده کنید . دستگاه های ATM مستقل (آنهایی که در بانک نیستند) آسان تر مورد هک قرار میگیرند.

هنگام اخذ پول نقد در تعطیلات آخر هفته باید بسیار مراقب باشید . سارقین تمایل به نصب دستگاه های هک کننده در آخر هفته ها دارند . زمانی که مطمئن شوند که بانک در ۲۴ ساعت آتی تعطیل است .

صورت حساب بانکی خود را مرتبا دنبال کنید و هرگونه برداشت غیر مجاز را سریعا گزارش کنید .

گردآورنده: حسین علیمرادی

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 نادری

محسن یزدی‌نژاد

فاطمه الهی

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/

کانال مرکز آپا خوارزمی:

@khu_cert

دانلود رایگان:

دانلود رایگان مجموعه کامل خبرنامه‌ها از طریق اسکن کد زیر در دسترس است.