شماره هفتم - مرداد ۱۳۹۶

خبرنامه "آپا" دانشگاه خوارزمی

در این شماره خواهید خواند:

چندین آسیب پذیری شدید و متوسط در کنسول SEC

ماه گذشته Cisco مشتریان را از چندین آسیب پذیری شدید و متوسط که توسط تحقیقات در کنسول SEC در زیرساخت نخستش پیدا شده بودند آگاه کرد - صفحه ۲

SLocker!

محققان امنیتی TrendMicro اعلام کرده اند اخیرا مشاهده شده Android file-encrypting ransomware Slocker با استفاده از یک رابط شبیه به بدافزار WannaCry ماه گذشته به سیستم های اندروید سراسر جهان ضربه زده است- صفحه ۳

اندروید و بدافزار SpyDealer

گونه‌ی جدید بدافزاری در اندروید که داده-های مربوط به بیش از ۴۰ اپلیکیشن ارتباطی از جمله WhatsApp، FaceBook و Skype را استخراج می‌کند. این بدافزار با استفاده از نرم افزار Baidu Easy Root گوشی مورد نظر را روت می‌نماید. - صفحه ۴

بدافزار GhostCtrl و ترکیبش با تروجان

تروجان‌های کنترل از راه دور یا RATها چیز جدیدی نیستند. این بخش از بدافزارها نزدیک به یک دهه است که موجودند و به خلافکاران از طریق درب پشتی دسترسی از راه دور می‌دهند. این حملات به کامپیوترها و کل شبکه‌ی شرکت برای سرقت اطلاعات، نصب بدافزار و انجام سایر اعمال خرافکارانه می‌باشد. تهدیدات مربوط به این بدافزار به آرامی در سیستم عامل اندروید در حال گسترش می‌باشد.- صفحه ۵

باج افزار Ceber علاوه بر کیف پول بیت کوین، پسورد آن را نیز به سرقت می‌برد.

باج افزار Cerber بر بازار باج افزارها تماما غالب می‌باشد. این باج افزار توسط سازندگان آن مرتبا آپدیت می‌شود و ویژگی‌های جدید به آن اضافه می‌گردد. همچنین این باج افزار به عنوان یک سرویس به هکرهای پایین رده برای کسب مقداری درآمد از طریق باج است. - صفحه ۶ و ۷

وقتی باب اسفنجی تقاضای باج می‌کند!

محققان امنیتی یک باج افزار بیت کوین را بر اساس یک شخصیت کارتونی به نام باب اسفنجی که در زیر دریا زندگی می‌کنند را شناسایی کردند. برطبق گزارشات در ۳۰ جولای ورژن ۲ باج افزار باب اسفنجی همچنان در حال توسعه بوده و به سختی فایل را رمزگذاری می‌کند. - صفحه ۸

چندین آسیب پذیری شدید و متوسط در کنسول SEC

ماه گذشته Cisco مشتریان را از چندین آسیب پذیری شدید و متوسط که توسط تحقیقات در کنسول SEC در زیرساخت نخستش پیدا شده بودند آگاه کرد و محصولات مدیریتی قابل برنامه ریزی (Programmable) را بهبود داد.

Cisco به کابران هشدار داده دستگاههایی که نرم افزارهای شرکتی IOS یا iOS XE را اجرا میکنند متاثر از چندین آسیب پذیری هستند که میتوانند برای اجرای از راه دور کد و حملات denial-of-service (DoS) اکسپلویت شوند.

نقص ها امنیتی شامل تزریق SQL، XML با ماهیت خارجی (XXE)، دیسکلوژر فایل لوکال و ضعف های اسکریپت کراس سایت (cross-site) است که میتواند از راه دور توسط مهاجمان معتبر یا غیر معتبر اکسپلویت شود.

مجموعا نه نقص امنیتی بر روی اجزاء پروتکل SNMP نرم افزارهای iOS و iOS XE اثر میگذارد. Patch هایی که ساخته میشوند هنوز به وسیله ی Cisco در

دسترس هستند اما این شرکت راه حل هایی را منتشر کرده است . یک مهاجم معتبر که تنها رشته ارتباطی SNMP سیستم هدف را میداند میتواند کد را اجرا کند یا باعث شود که دستگاه با فرستادن بسته های SNMPطراحی شده از طریق IPv4 یا IPv6، مجددا بارگذاری شود.

اگر مهاجم بتواند کد را اجرا کند، ممکن است بتوانند کنترل تمامیت سیستم آسیب دیده را بدست بگیرد. آسیب پذیری هایی که بر دستگاه های iOS اثر میگذارد اگر با یکی از نه پایگاههای اطلاعات مدیریتی (MIBs) تنظیم و هماهنگ شود هر نسخه از SNMP را اجرا می کنند که به سازمان ها اجازه ی مدیریت مانند روترها یا سویچ ها در شبکه را میدهد. Cisco میگوید این حفره های امنیتی را در طول آزمایش داخلی پیدا کرده است اما کمپانی به مشتریان هشدار میدهد که اشخاص حقیقی بیرون از شرکت ، در مورد آسیب پذیری ها اطلاعات دارند که این شانس اکسپلویشن را افزایش میدهد.

یک توصیه نامه توسط کنسول SEC منتشر شده است که شامل کد اثبات مفهوم (PoC) برای هر آسیب پذیری میباشد. در حالی که Cisco در مورد چنین نشریاتی در نوامبر ۲۰۱۶ اطلاع داده بود، انتشار پچ ها را چندین بار به تعویق انداخته است. Patch ها بالاخره هفته پیش در دسترس قرار گرفت.

گردآورنده: حسین علیمرادی

SLocker!

محققان امنیتی TrendMicro اعلام کرده اند اخیرا مشاهده شده Android file-encrypting ransomware Slocker با استفاده از یک رابط شبیه به بدافزار WannaCry ماه گذشته به سیستم های اندروید سراسر جهان ضربه زده است. Slocker یکی از اولین خانواده ی بدافزارهای اندروید برای رمزگذاری فایل ها روی دستگاههای به خطر افتاده که مدتی قبلا موفقیت کوتاه داشته است . مسئول آن به عنوان مظنون پنج روز بعد از ردیابی اولیه دستگیر شد.

این بدافزار در ابتدا تعداد کمی از کابران رااز طریق کانال های انتقال محدود (فروم هایی مثل گروههای QQ و سیستم های Bulletin Board) آلوده کرد، اما در پی تلاش برای انتشار موفقیت آمیز WannaCry است. Trend Micro مینویسد نمونه ی اوریجینال ransomware که اوایل این ماه پیدا شد King of Glory Auxiliary نامیده شده و قرار بود به عنوان ابزار تقلب برای بازی King of Glory باشد. پس از نصب Ransomware ظاهری شبیه به WannaCray داشت.

برای تطمیع کابران به نصب آن، SLocker Ransomware به شکل ویدئو پلیر و سایر انواع برنامه ها مخفی میشود. بعد از اینکه اپلیکیشن برای اولین بار اجرا شد، آیکون و نام آن همراه با والپیپر دستگاه آلوده تغییر میکند. همچنین این بدافزار چک میکند که آیا قبلا اجرا شده و اگر اجرا نشده باشد یک عدد رندوم تولید میکند و آن را در SharedPreferences ذخیره میکند. در

مرحله ی بعد threat دایرکتوری حافظه ی خارجی دستگاه را تعیین موقعیت میکند و thread جدید را شروع میکند که ابتدا از طریق دایرکتوری میرود تا به فایل هایی که نیازهای خاص را برآورده میکند را پیدا کند.

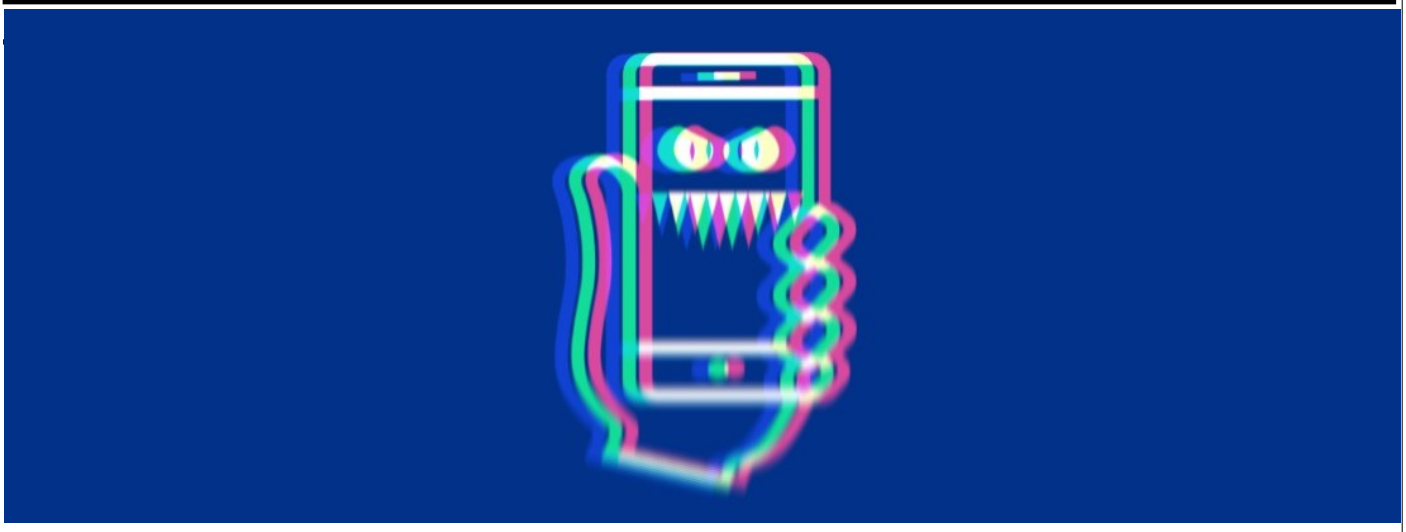
محققان امنیتی می‌گویند "ما میبینیم که ransomware از رمزگذاری فایل های سیستمی اجتناب میکند، روی فایل های دانلود شده و عکس ها تمرکز میکند و تنها فایل هایی را که پسوند دارند (فایل های متنی، تصاویر، ویدئو ها) را رمز گذاری میکند. وقتی که یک فایل که نیازهای خاص را برآورده میکند پیدا شد Thread از ExecutorService برای اجرای وظیفه جدید استفاده خواهد کرد".

بدافزار یک رمز براساس عدد رندومی که قبلا تولید کرده بود تولید میکند و رشته را برای ایجاد کلید نهایی برای AES قبل از استفاده از AES برای رمزگذاری فایل ها، تامین میکند. قربانیان Slocker سه آپشن برای پرداخت جبران خسارت دارند، اما هرسه به یک کد QR یکسان ختم میشود که از قربانیان میخواهد با سرویس پرداخت موبایل چینی محبوب QQ پرداخت کنند. بدافزار همچنین قربانیان را تهدید میکند که مقدار Ransom بعد از سه روز افزایش خواهد یافت و فایل ها بعد از یک هفته پاک خواهند شد. آنالیز malware نشان داده که کلید رمزگشایی با value در MainActivity.m مقایسه میشود که عدد تصادفی از قبل تولید شده به علاوه ی ۵۲۰ است. TrendMicro مینویسد کاربران اگر بتوانند روشی برای تولید کلید رمزگذاری پیدا کنند میتوانند فایل هایشان را به صورت رایگان رمزگشایی کنند .

TrendMicro مینویسد در مقایسه با Ransomware که قبلا دیده ایم این Ransomware نسبتا ساده است. برای یک مهندس امنیت معکوس سازی Ransomware و پیدا کردن روشی برای رمزگشایی فایل ها کار خیلی ساده ای است. با این حال تکثیر گونه های جدید به صورت خیلی سریع بعد از اولین آنها نشان میدهد این بازیگران مخرب تضعیف نمیشوند. است . برای در امنیت و محافظت ماندن، کاربران باید تنها اپلیکیشن ها را از AppStore های قانونی و معتبر دانلود کنند و مجوزهایی را که توسط هر اپلیکیشن درخواست میشود چک کنند خصوصا وقتی که به نرم افزار اجازه ی خواندن/نوشتن روی حافظه ی خارجی را میدهد. کاربران باید از دیتاهای خود به صورت منظم بک آپ بگیرند و یک آنتی ویروس جامع و کامل را به عنوان یک راه حل، نصب و نگهداری کنند.

گردآورنده: حسین علیمرادی

اندروید و بدافزار SpyDealer



گونه‌ی جدید بدافزاری در اندروید که داده‌های مربوط به بیش از ۴۰ اپلیکیشن ارتباطی از جمله WhatsApp، FaceBook و Skype را استخراج می‌کند.

Unit 42، دپارتمان هوشمند تهدیدات شبکه‌ای Palo Alto، تهدید جدیدی را با نام SpyDealer کشف نموده است که گفته می‌شود پیغام‌ها و سایر اطلاعات شخصی شامل مشخصات مخاطبین به وسیله‌ی Exploit سرویس دسترسی در اندروید را سرقت می‌برد. این بدافزار همچنین قابلیت ضبط تماس‌ها، صدا و تصویر اطراف و موقعیت مکانی را دارا می‌باشد. همچنین این بدافزار قابلیت عکسبرداری با استفاده از دوربین دستگاه را دارا می‌باشد.

این بدافزار با استفاده از نرم افزار Baidu Easy Root گوشی مورد نظر را روت می‌نماید. بیشتر اپلیکیشن‌هایی که SpyDealer داده‌های آنان را به سرقت می‌برد دارای قابلیت رمزنگاری end-to-end می‌باشند. توسعه‌دهندگاه این بدافزار با استفاده از امتیازات دسترسی روت وبا پیاده سازی سرویس دسترسی اضافه قادر به دزدین متن‌های غیر رمزنگاری به طور مستقیم و با استخراج آنان از صفحه‌ی برنامه‌های ارتباطی می‌باشند.

این برنامه از طریق Google Play پخش نشد است اما وجود آن به گوگل گزارش شده است. Unit 42 همچنان مطمئن نیست که این بدافزار چگونه کاربران را آلوده کرده است اما شواهدی مبنی بر اجرای این بدافزار بر شبکه‌های بیسیم در چین موجود است. تمامی ۸۸ سرور کنترل و فرمان‌دهنده این بدافزار در چین قرار دارد به جز ۳ تای آن که در آمریکا می‌باشد. خبر خوب این است که این بدافزار تنها برروی ورژن‌های قدیمی اندروید (از ۲.۲ تا ۴.۴) تاثیر گذار بوده و از این شمار تنها آنانی که قابلیت اجرای Baidu Easy Root را دارا می‌باشند. SpyDealer قابلیا تاثیرگذاری برروی ورژن‌های جدیدتری از اندروید را می‌باشد اما نمی‌تواند اقداماتی را که نیاز به امتیازات بالاتر است انجام دهد.

Unit 42 بیش از ۱۰۰۰ نمونه از SpyDealer (با نام GoogleService یا GoogleUpdate) یافته است. اولین مورد در اکتبر ۲۰۱۵ مشاهده گردید و آخرین آن در می ۲۰۱۷. این شرکت ۳ نسخه متفاوت از این بدافزار یافته است که این امر یعنی این بدافزار همچنان در حال توسعه می‌باشد.

گردآورنده: محمد مرتضوی

بدافزار GhostCtrl و ترکیبش با تروجان

تروجان‌های کنترل از راه دور یا RATها چیز جدیدی نیستند. این بخش از بدافزارها نزدیک به یک دهه است که موجودند و به خلافکاران از طریق درب پشتی دسترسی از راه دور می‌دهند. این حملات به کامپیوترها و کل شبکه‌ی شرکت برای سرقت اطلاعات، نصب بدافزار و انجام سایر اعمال خرافکارانه می‌باشد. تهدیدات مربوط به این بدافزار به آرامی در سیستم عامل اندروید در حال گسترش می‌باشد.

این RAT جدید در اندروید که همانند یک کنترل از راه دور عمل می‌کند، نام GhostCtrl بر آن گذاشته شده است. تروجان‌ها به اندازه‌ی کافی آزار دهنده هستند اما GhostCtrl ترفندی جدید در آستین دارد. نه تنها آن موبایل را با ریست کردن PIN کدها قفل می‌کند و اطلاعات را به سرقت می‌برد، بلکه به عنوان یک باج افزار نیز عمل می‌کند. فرد قربانی یک پیغام مبنی بر پیام باج افزار زمانی که به RAT آلوده شده است را می‌بیند.

خوشبختانه به نظر می‌رسد که GhostCtrl در حال حاضر به طور فعال به عنوان باج افزار توزیع نشده است. تمامی دستگاه‌هایی که تا امروز به این بدافزار آلوده شده‌اند داده‌هایشان نظیر پیام‌های متنی، مخاطبین و غیره دزدیده شده است. محققان حداقل یک نمونه کاری از این بدافزار را دریافته‌اند و سورس کد این بدافزار قابلیت‌های بعدی آن را به وضوح نشان می‌دهد. این چشم انداز تا حدودی نگران کننده است که به عنوان باج افزار موبایل، تاکنون چنین بازار بزرگ منحصر به فردی به نمایش گذاشته نشده بود.

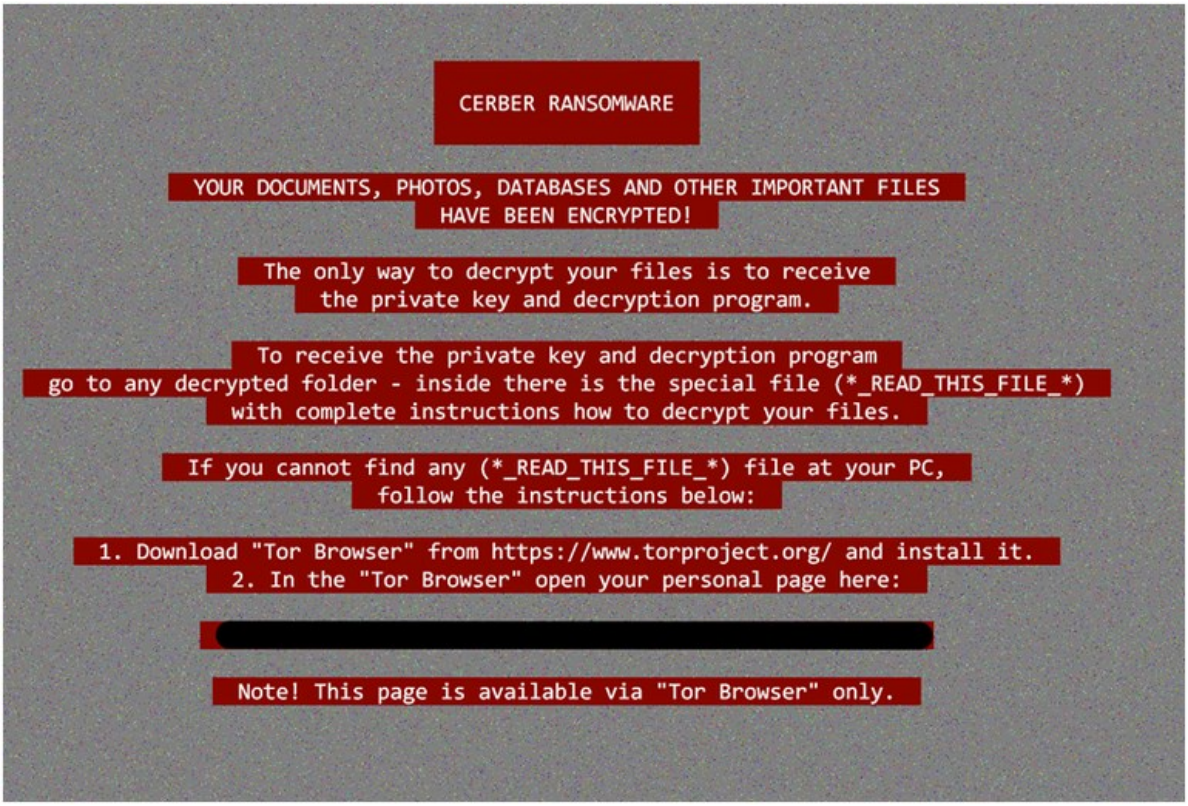
چیزی که تروجان با دسترسی از راه دور را بسیار دردسر ساز می‌کند این است که آن نیز خودش بخشی از یک بدافزار می‌باشد. OmniRAT قابلیت حمله به دستگاه‌هایی با یکی از چهار سیستم عامل بزرگ را دارد. این RAT خاص می‌تواند سیستم عامل اندروید، MacOS، Linux و ویندوز را آلوده نماید به همین جهت یکی از مهم‌ترین خطرات سایبری تاریخ به شمار می‌رود. به نظر می‌رسد که GhostCtrl بر پایه‌ی OmniRAT باشد و تولید آن توسط توسعه دهندگانی که به ابزارهای این بدافزار که به عنوان سرویسی برای سایر بدافزارها برروی پورتال Darknet قرار دارد صورت گرفته باشد.

اگرچه GhostCtrl هنوز به عنوان یک باج افزار مورد استفاده قرار نمی‌گیرد اما این بدافزار به شامل ابزارهایی قدرتمند با ویژگی-هایی خاص می‌باشد. برای نمونه، این بدافزار قابلیت روت کردن گوشی آلوده، کنترل توابع ویبره گوشی، پاک کردن و تغییر نام دادن فایل‌ها، ارسال SMS و MMS و قطع ارتباطات را دارد. تمامی این فعالیت‌ها علاوه بر قابلیت جمع آوری داده در این بدافزار انجام می‌گیرد که در آن تاریخچه تماس‌ها، شماره تلفن‌ها، نام‌های کاربری، پسوردها و داده دوربین مورد هدف قرار گرفته است.

GhostCtrl یکی از اولین بدافزارهایی است که از روش دوگانه در یک پکیج استفاده می-کند. اگرچه این RAT سیستم عامل اندروید را مورد هدف قرار می‌دهد اما سورس کد این باج افزار نشان می‌دهد که به راحتی قابل انتقال به سایر سیستم عامل‌ها است. این پکیج‌های باج افزاری که از چندین بدافزار تشکیل شده‌اند در آینده خطرات امنیتی بسیاری از جمله آلودگی باج افزاری و حملات DDoS براساس IoT به وجود خواهند آورد.

گردآورنده: محمد مرتضوی

باج افزار Ceber علاوه بر کیف پول بیت کوین، پسورد آن را نیز به سرقت می‌برد.



یکی از بدترین نوع باج افزار که به نامطبوع‌ترین آنان نیط تبدیل شده است، علاوه بر قابلیت به سرقت بردن کیف پول بیت کوینی و پسورد اطلاعات از قربانی، فایل‌ها را رمزنگاری کرده و برای بازگرداندن آنان درخواست باج می‌کند.

باج افزار Cerber بر بازار باج افزارها تماما غالب می‌باشد. این باج افزار نه تنها توسط سازندگان آن مرتبا آپدیت می‌شود و ویژگی‌های جدید به آن اضافه می‌گردد، همانند قابلیت مخفی شدن از ابزار تشخیص دهنده‌ی سایبری. همچنین سازندگان این باج افزار آن را به عنوان یک سرویس به هکرهای پایین رده برای کسب مقداری درآمد از طریق باج می‌فروشند.

همه چیز از آنجایی سخت‌تر می‌شود که باج افزار از رمزنگاری بسیار قوی استفاده می‌کند و طبیعت در حال توسعه‌ی این باج افزار نشان دهنده‌ی این است که هیچ ابزار رمزگشایی برای آخرین ورژن آن موجود نیست.

آخرین فرضیه‌ها از باج افزار Ceber نشان می‌دهد که این باج افزار پول دیجیتال و پسورهای قربانی را به سرقت می‌برد و یک سود اضافی بر روی مقدار آن چیزی که باج می‌گیرد، مبلغی از ۳۰۰ تا ۶۰۰ دلار را درخواست می‌کند.

متد انتشار این باج افزار همانند قبل بوده و با پیوست شدن به ایمیل‌های فیشینگ به قربانی حمله می‌کند. اما کیت مربوط به Exploit شامل بدافزارها و نرم افزارهای خرابکارانه‌ی دیگری می‌باشد که قبل از اجرای فرآیند رمزنگاری، اجرا می‌گردند.

محققان TrendMicro بیان نمودند که حمله‌ی نسبتا ساده‌ای از سوی باج افزار Cerber سه اپلیکیشن مربوط به کیف بیت کوین را هدف قرار می‌دهدکه عبارتند از برنامه‌های Bitcoin Coin و اپلیکیشن‌های واسط کیف پول‌های Electrum و Multibit.

برای دسترسی به محتوای کیف پول نیاز به یک پسورد می‌باشد اما Cerber این مشکل را نیز حل کرده است. این باج افزار پسوردهای ذخیره شده در Internet Explorer، Google Chrome و Mozilla Firefox را به سرقت می‌برد.

ادامه در صفحه ی بعد.

گردآورنده: محمد مرتضوی

باج افزار Ceber علاوه بر کیف پول بیت کوین، پسورد آن را نیز به سرقت می‌برد

اطلاعات مربوط به هر پسورد ذخیره شده در خصوص کیف پول بیت کوین برای حمله کننده از طریق سرور فرمان و کنترل ارسال می‌شود و باعث می‌شود هکر به محتوای داخل پول مجازی دسترسی پیدا کند.

برای افزایش ضرر و صدمه، باج افزار فایل‌های مربوط به کیف پول را قبل اط شروع فرآیند رمزگذاری پاک می‌کند و درخواست مبلغی قابل تبدیل برای باز گرداندن فایل‌ها می‌کند.

Gilbert Sison و Janus Agcaoili، دو محقق از TrendMicro همچنین بیان کردند: "این ویژگی جدید نشان می‌دهد که حمله کنندگان در حال سعی و کوشش برای دستیابی به یک راه جدید برای کسب درآمد از باج افزار می‌باشند. دزدیدن بیت کوین‌های کاربر هدف یک منبع درآمد بالقوه می‌باشد."

Cerber اولین خانواده از باج افزارها نمی‌باشد که اطلاعات قربانی را به سرقت می‌برد اما این امر باعث نگرانی است که فرم رایجی از باج افزارها در حال تطبیق با این تکنیک هستند.

از زمانی که Cerber این ویژگی‌های جدید را اضافه نموده است، آموزش کاربران برای هوشیاری در برخورد با پیوست‌های مشکوک در ایمیل یا منابع غیر قابل تایید یکی از بهترین روش‌ها برای دوری از آلودگی است.

در حالی که هویت باند هکر پشت سر باج افزار به صورت یک رمز باقی مانده است، اما تکامل مستمر و توسعه‌ی آن به نظر می‌رسد یک عملیات سازمان یافته می‌باشد.

گردآورنده: محمد مرتضوی

وقتی باب اسفنجی تقاضای باج می‌کند!

همانطور که در این ماه مشخص است، بازار باج افزارها همچنان داغ می باشد و هرکسی با هر سطح اطلاعاتی سعی دارد تا باج افزار خود را طراحی و در شبکه‌ی اینترنت گسترش دهد. از طرفی هم استفاده از اسم‌های مختلف که باعث جلب توجه افراد می‌شود یکی دیگر از حقه‌هایی است که این طراحان باج افزار به کار می‌گیرند.

موفقیت در بازار باج افزار یکی از راحت‌ترین راه‌های کسب پول و بیت کوین بوده و هر فردی که بتواند باج افزار خودرا به هر نحوی که شده بیشتر گسترش دهد، توانایی کسب باج بیشتری را هم خواهد داشت.

محققان امنیتی یک باج افزار بیت کوین را بر اساس یک شخصیت کارتونی به نام باب اسفنجی که در زیر دریا زندگی می‌کنند را شناسایی کردند.

برطبق گزارشات در ۳۰ جولای ورژن ۲ باج افزار باب اسفنجی همچنان در حال توسعه بوده و به سختی فایل را رمزگذاری می‌کنند. Karsten Hahn تحلیل گر G Data نیز در توییت خود اعلام کرد که این باج افزار یا

در مرحله‌ی تست می‌باشد و یا اینکه تنها یک شوخی از سوی توسعه دهندگان بوده. این نسخه دارای قابلیت پیش نمایش فایل-های رمزگذاری شده را نیز دارد.

علیرغم کمبودهای قابل توجه آن، محققان می‌گویند این باج افزار از راهکار WannaCry برای استفاده از همان لایه‌ی باج افزاری اما با شکل و ظاهر باب اسفنجی استفاده می‌کند.

اطلاعات کمی در خصوص ورژن ۱ موجود است، که آن یک نسخه‌ی ناموفق بوده و به مرحله‌ی توزیع نرسیده است. همچنین محققان بیان نموده‌اند که قطعی نیست که نسخه‌ی پیشین این باج افزار انتشار یافته باشد. اگرچه این باج افزار باعث بحث و تبادل نظر محققان در خصوص هدف این باج افزار نشده است، استفاده از یک برند شناخته شده‌ی جهانی و ارتباط آن با نرم افزارهای خرابکارانه به سرعت باعث جلب توجه رسانه‌ها شده است.

هنوز تعدا زیادی از این بدافزارها و باج افزارهای صنعتی موجود است. همه‌ی پروژهای بزرگ درحال توسعه باعث ایجاد خسارات بزرگ نخواهند شد اما نشان می‌دهد که هرکس می‌تواند محتوای موجود را فراهم و آن را به راحتی به چیزی خرابکارانه تبدیل کند.

گردآورنده: محمد مرتضوی

Kharazmi CERT Coordinator Center

مرکز آپا دانشگاه خوارزمی

نشانی:

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

رییس مرکز:

دکتر امید مهدی عبادتی

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

اعضای هیات علمی:

دکتر احسان ملکیان

دکتر امید مهدی عبادتی

وب سایت:

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

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

محسن یزدی نژاد