شماره ششم - تیر ۱۳۹۶

خبرنامه "آپا" دانشگاه خوارزمی

در این شماره خواهید خواند:

هشدار! هکرها استفاده از SambaCry را برای هک سیستم های لینوکس شروع کردند.

دو هفته پیش گزارشی در خصوص یک کد آسیب پذیری اجرایی بحرانی مربوط به ۷ سال گذشته در نرم افزار شبکه ی Samba (یک پیاده سازی از پروتکل شبکه ای SMB) انتشار یافت که به هکرها قابلیت کنترل کامل یک کامپیوتر آسیب پذیر با سیستم عامل Linux و Unix را می دهد.

برای اطلاع از آسیب پذیری مربوط به SambaCry و همچنین اطلاع از عملکرد آن به کد آسیب پذیری CVE-2017-7494 مراجعه شود.

در همین لحظه نزدیک به ۴۸۵۰۰۰ کامپیوتر با Samba های فعال تشخیص داده شده است که در معرض خطر در اینترنت موجودند و محققین پیش بینی می کنند که حملات SambaCry قابلیت گسترشی مشابه باج افزار WannaCry را خواهند داشت.

گزارشات استخراجی دقیق، از Honeypot های نصب شده توسط تیم تحقیقاتی Kaspersky وجود بدافزاری که بهره برداری از آسیب پذیری SambaCry را برای آلوده کردن کامپیوترهای لینوکسی مهیا می کند، با نرم افزار cryptocurrency mining مشخص کرده است.

یک محقق امنیتی دیگر به نام Omri Ben Bassat، به طور مستقل این مورد را کشف نموده و نام آن را EthernalMiner گذاشته است.

بر طبق تحقیقات، یک گروه ناشناس از هکرها، دزدی از کامپیوترهای لینوکس را تنها یک هفته بعد از اینکه جریان Samba به طور عمومی فاش شد شروع کردند و در نهایت اقدام به نصب و به روز رسانی ورژنی از CPUminer کردند که یک نرم افزار cryptocurrencyبرای جمع آوری پول دیجیتال Monero می باشد.

بعد از به خطر انداختن کامپیوترهای آسیب پذیر توسط SambaCry، هکرها ۲ مورد را برروی کامپیوترهای قربانی به اجرا گذاشتند:

INAebsGB.so یک معکوس کننده ی Shell که دسترسی به حمله کننده را ایجاد می کند

cblrwuocc.so یک درب پشتی که شامل ابزارهای cryptocurrency می باشد – CPUminer

همچین شرکت Kaspersky اعلام کرد: زمانی که INAebsGB.so برروی کامپیوتر قربانی اجرا می شود، حمله کننده قابلیت تغییر تنظیمات نرم افزار جمع آوری کننده ی پول دیجاتال که از قبل برروی کامپیوتر قربانی نصب و اجرا شده است را دارد.

نرم افزار جمع آوری cryptocurrencies نیاز به مقدار زیادی از منابع محاسباتی و کامپیوتری برای جمع آوری پول دیجیتال دارد، اما با استفاده از بد افزار جمع آوری cryptocurrencies، یک مجرم سایبری می تواند به راحتی و با استفاده از منابع موجود در کامپوترهای قربانبان خود اقدام به جمع آوری پول دیجیتال نماید.

همانطور که قبلا نیز در خبرگزاری ها مطرح شد، Adylkuzz که بد افزار جمع آوری cryptocurrencies از آسیب پذیری SMB در ویندوز می باشد که حداقل ۲ هفته قبل از باج افزار WannaCry شیوع پیدا کرد.

بدافزار Adylkuzz یک نرم افزار جمع آوری کننده ی Monero می باشد که این کار را با استفاده از مقدار زیادی از منابع محاسباتی سیستم عامل ویندوز انجام میدهد.

حمله کنندگان موجود در پشت SambaCry-based CPUminer تا کنون ۹۸ XMR جمع آوری کرده اند که ارزش آن معادل ۵۳۸۰ دلار می باشد. همچنین با رشد کامپیوترهای آلوده شده این مقدار رشد بیشتری خواهد داشت.

در روز اول آنان در حدود۱ XMR (در حدود ۵۵ دلار) جمع آوری کردند. اما در طول هفته ی گذشته ی آن ها در هر روز ۵ XMR جمع آوری کرند.

توسعه دهندگان Samba برای این موضوع وصله ی نرم افزاری در ورژن های جدید آن ۴.۶.۴، ۴.۵.۱۰، ۴.۴.۱۴ ارائه نمودند و از دارندگان آن درخواست کردند تا حتما این وصله ی نرم افزاری را نصب نمایند.

گردآورنده: محمد مرتضوی

Koler باج افزاری برای کاربران اندوید امریکایی

باج افزار دیگری به نام Koler کاربران امریکایی را با تبلیغات جعلی یک نرم افزار مربوط به یکی از سایت "های غیراخلاقی" آلوده می کند.

طبق آخرین اخبار ورژن های متفاوتی از این باج افزار با قابلیت موقعیت جغرافیایی در نمایش تبلیغات به زبان های مختلف براساس موقعیت مکانی کاربران وارد امریکا شده است.

همانند سایر حملات این چنینی، کاربران را با نمایش محتوای غیراخلاقی جذب و آنان را ترقیب به دانلود و نصب اپلیکیشن های سایت های غیر اخلاقی می کند. به محض دانلود این باج افزار و با استفاده از کلیک کاربر، این باج افزار دسترسی مدیر سیستم را به خود می دهد.

سپس Koler با استفاده از این سطح دسترسی یادداشت های باج گیرانه خود را به نمایش می گذارد و در بالای صفحه یک هشدار FBI در خصوص فایل های مشکوک برروی کامپیوتر فرد مورد نظر می دهد. محققان امنیتی گفته اند که قفل صفحه گوشی کاربر را می توان به وسیله ی Boot دستگاه در حالت Safe Mode پاک کرد و همچنین می توان با پاک کردن این نرم افزار تقلبی، این باج افزار را از روی دستگاه پاک نمود.

اگرچه غیرفعال کردن باج افزارهای این چنینی برای محققان امنیتی کار بسیار ساده ای است اما مردم باید بدانند که دانلود از منابع مشکوک باعث رخداد چنین حملاتی خواهد شد.

Zeltser گفته است: "بله، مردم نباید هر اپلیکیشنی را از فروشگاه های نرم افزاری نامعتبر دانلود نمایند. بنابراین، بهتر است به خاطر داشته باشیم که بیشتر افراد غیر متخصص در حوضه های امنیتی فرق یک فروشگاه نرم افزاری با سایر آنان را نمی دانند و نمی توانند تفاوت بین یک برنامه ی مخرب و یک برنامه ی کاربردی را تشخیص دهند".

وی همچنین این مطلب را بیان نمود که چگونه می توان تنظیمات امنیتی در وسیله های نقطه پایانی را تقویت کرد تا مردم از صدمه دیدن درمقابل چنین بدافزارهایی مقاوم شوند و چگونه کنترل های امنیتی تنظیم گردد تا بدافزارها بدون دخالت در فعالیت های نرمال و طبیعی سازماندهی شوند.

Wenzler استراتژیست امنیت عمومی AsTech همچنین بیان کرد: "موفقیت بدافزارهایی همچون Koler، با وجود تمام هشدارهایی که مردم را از کلیک کردن برروی لینک های نامعتبر یا دانلود اپلیکیشن های غیر معتبر منع می کند دو موضوع اصلی را مشخص می کند. اول درصد پایین موفقیت حمله تا برای حمله کننده منفعتی را ایجاد کند. دوم اینکه اکثر کاربران در امریکا کمتر در خصوص خطرات این بدافزارها نگران هستند."

خیلی از کاربران خطر واقعی کلیک برروی لینک های آلوده ویا دانلود اپلیکیشن ها را جدی نمی گیرند زیرا آنان اهمیتی به فروشگاه نرم افزاری سیستمشان نمی دهند و یا اینکه برای افزایش میزان سطح کاربریشان - در این خصوص، دسترسی به اکانت های رایگان کاربری سایت های غیر اخلاقی و محتوای آنان- ممکن است تا این اعمال را انجام دهند.

Abhishek Singh مدیر ارشد Acalvio بیان کرد: باج افزار ها از روش های تکنیکی خاصی برای فرار و دور زدن سیستم های امنیتی سنتی استفاده می کنند که می توان آن را به مسابقه ی تسلیحاتی توصیف نمود، تخمین زده می شود که مجموع خسارات ناشی از باج افزارها در سال ۲۰۱۷ به مقدار ۵ میلیارد دلار می باشد.

Singh همچنین بیان کرد که استفاه از ابزارهای مربوط به deception-centric برای تشخیص باج افزارها بر سیستم های تشخیص دهنده ی سنتی برای ارگان ها بسیار مهم می باشد.

گردآورنده: محمد مرتضوی

یک حمله ی باج افزاری با Petya

هکرها بانک مرکزی اوکراین، سازمان نیرو، یک فرودگاه و شماری از آژانس ها و کمپانی ها را با حمله ی باج افزاری (سه شنبه ۶ تیر) مورد هدف قرار دادند. این عمل باعث شد تا شمار زیادی از مقامات نتوانند به کامپیوترهای خود دسترسی داشته باشند و طبق گفته ها شماری از شهروندان نتوانند به حساب های پولی خود دسترسی پیدا کنند. اما بخش ترسناک آن اینجاست که ایالات متحده قرار است هدف بعدی باشد.

از زمان شروع حملات باج افزاری بیش از ۸۰ کمپانی در اوکراین، روس، انگلیس و هند مورد حمله قرار گرفته اند. هکرها برای بازگشایی کامپیوترهای رمزنگاری شده درخواست ۳۰۰ دلار به واحد بیت کوین را دارند. یکی از نمایندگان شرکت برق Kyivenergo به Interfax (آژانس خبری اوکراین) گفته است که این کمپانی تمامی کامپیوترهای خود را بعد از حمله خاموش کرده است و آنان منتظر اجازه ی سرویس امنیتی اوکراین هستند تا دوباره کامپیوترها را روشن نمایند.

در همین حال، Anton Gerashchenko، دستیار وزیر کشور، در پست فیس بوک خود این حمله را بزرگترین حمله تاریخ به کشور اوکراین دانست. او همچنین ادعا کرد که: این عمل یک کار مخفی برای اخاذی می باشد. اما در حقیقت هدف بی ثبات کردن وضعیت اقتصادی و اجتماعی اوکراین می باشد. که در هدف اخیر از حمله ی سایبری اتفاق افتاده این حرف کاملا منطقی است.

قبل از اینکه وارد پیامدهای جغرافیایی شویم، بهتر است در مورد این باج افزار صحبت کنیم. سازمان آنالیز و گزارش سوییس برای تضمین اطلاعات (MELANI) مشخص کرده که باج افزار با عنوان Petya، یک صلاح سایبری می باشد که پیش از نیز دیده شده است. اگرچه در درجه ی اول هدف آن اوکراین می باشد، اما مقیاس آن با باج افزار WannaCry قابل قیاس است (باج افزاری که شمار زیادی کامپیوتر را در ماه می May از کار انداخت) مقایسه شده است. در این ماه، هر فرد از سازمان های دولتی اوکراین تا شرکت حمل و نقل دانمارکی Maersk به ظاهر که آلوده شده اند. لیست سازمان ها و ارگان های آلوده در هر ساعت در حال افزایش می باشد.

اخیرا اوکراین با حمله ی سایبری مواجه شده است که در دو سال گذشته بی سابقه بود است. با این حال، بعد از دو حمله ی متوالی سال گذشته که باعث از کار افتادن بخش هایی از برق پایتخت (Kive) این کشور شد، همچنین مشخص است که هکرها در حال افزایش تلاش خود هستند.

ادامه مطلب در صفحه ی بعد

گردآورنده: محمد مرتضوی

یک حمله ی باج افزاری با Petya (ادامه...)

زمان حمله ی روز سه شنبه نیز بسیار جالب است. رشته حملات درست چند ساعت بعد از کشته شدن افسر اطلاعاتی بلند پایه ی اوکراین در اتومبیل بمب گذاری شده در پایتخت شروع شد. برای ادعای این که این حوادث به یکدیگر متصل هستند فعلا بسیار زود می باشد اما روند حرکت به سوی جنگ های شدیدتر سایبری ناشی از درگیری ها موجود در منطقه غیر قابل انکار است.

خیلی ها، از جمله رییس جمهور اوکراین آقای Petro Porshenko، معتقد است که روس ها برای هدف قرار دادن اوکراین و تضعیف روند سیاسی، اقتصادی و زیرساخت های فیزیکی از هکرها حمایت می کند.

محور این حملات به سال ۲۰۱۴ برمی گردد، زمانی که در انقلاب اوکراین Viktor Yanukovych از قدرت حذف شد. بعد از آن، یک گروه هکر حرفه ای روسی به نام CyberBerkut برای راه اندازی انتخابات در اوکراین تلاش کردند. گروه نام برده با گروهی که به کمیته ملی دموکراتیک (DNC) در انتخابات ۲۰۱۶ آمریکا نفوذ کردند ارتباط دارند.

تحقیقات ارتباط یک گروه از هکرهای روسی با نام Sandworm را با BlackEnergy، یک مجموعه مخرب از بدافزارها را که نه تنها برروی کامپیوترهای شرکت های اوکراین بلکه برروی شبکه ی آب و برق ایالات متحده ی امریکا موجود است را نشان می دهد.

تحقیقات امنیتی Dragos نیز همچنین گروه هکری Sandworm را با CrashOverride در ارتباط دانسته است. CrashOverride صلاح سایبری فوق العاده قدرتمند چند منظوره ایست که در خلال خاموشی شدن Kiev در سال ۲۰۱۶ مورد استفاده قرار گرفت.

اگر در ذهن خود شروع به در حال چرخیدن میان این ارتباطات آشفته در حمله ی سایبری اوکراین و پتانسیل حمله ی فاجعه بار به زیر ساخت های ایالات متحده هستید نکته دقیقا همین جاست. تمامی این قضایا بسیار ترسناک می باشد. همانند فیلم هالیوودی BlackHat اما ۱۰۰ برابر ترسناکتر با تسلیحات سایبری واقعی و پیچیده تر هستند.

دوباره یادآور می شویم که ارتباط روس ها با این حملات همچنان مشخص نمی باشد. محققان امنیتی در حال کشف روابط و بررسی کدها برای آشکار کردن این واقعیت هستند. همچنان لیست کشورهایی که به این باج افزار در حال آلوده شدن هستند به سرعت در حال افزایش است.

گردآورنده: محمد مرتضوی

ورژن جدید باج افزار CryptoMix با نام Azer

مدل های متفاوتی از باج افزارهای پول های دیجیتالی وجود دارد. بیشتر این باج افزار ها دارای پوسته کد متفاوت مربوط به خود می باشند. CryptoMix باج افزاری است که در سال گذشته به شهرت رسید و محققان امنیتی، نوع جدید آن را Azer نامیدند. این باج افزار خاص دارای چندین ویژگی جذاب می باشد که در ادامه به بررسی آنان خواهیم پرداخت.

Azer نژاد جدید و جالبی از باج افزارها می باشد.

تاکنون بدافزارها و باج افزارهای زیادی دیده شده اند. در اکثر موارد، انواع جدید این بدافزارها زندگی را برای قربانیان و محققان امنیتی بسیار دشوار کرده است. بازار باج افزار ها به رونق گرفتن خود در سال جاری ادامه می دهد. ماهانه تعداد تهدیدات افزایش پیدا می کند که این موارد تنها باعث ایجاد دردسرهای بیشتر است.

باج افزار Azer یک تصویر خوب از باج افزار CryptoMix می باشد که ما می توانیم در آینده انتظار داشته باشیم. باج افزار CryptoMix برای مدت زیادی است که در گردش قرار دارد و آخرین نسخه ی آن Azer با نمونه ای که در طول چندماه گذشته با آن کار شد دارای تغییرات جالبی می باشد.

در ابتدا، یادداشت های باج افزار Azer با چیزی که در باج افزار CryptoMix مشاهده شد متفاوت می باشد. نام آن تغییر کرده است و توضیحات خلاصه شده است. از قربانیان خواسته شده تا قبل از اینکه آنان بتوانند اطلاعات پرداخت را دریافت کنند، به حمله کننده ایمیلی ارسال کنند. این امر نشان می دهد که Azer از سرویس کنترل و فرمان استفاده نمی کند. این امر روندی جدید در میان باج افزارهایی است که تا سال ۲۰۱۷ مشاهده شده است.

Azer شاید یکی از اولین انواع باج افزار ها باشد که تماما به صورت آفلاین کار می کند. در حالی که تمامی باج افزار ها از سیستم ارتباطی آنلاین استفاده می کنند این امر غیر معمول است. دیدن این امر که یک باج افزار از ارتباط شبکه استفاده نمی کند کمی غریب به نظر می رسد اما ممکن است باعث ایجاد تغییر بزرگی در صحنه ی باج افزارها شود.

آفلاین کار کردن باج افزار Azer به این معنا نیست که شکستن رمزنگاری آن ساده می باشد. در حقیقت، در این بدافزار نزدیک به کلید عمومی جاسازی شده است. به هیچ عنوان مشخص نمی باشد که کدام کلید در رمزنگاری مورد استفاده قرار می گیرد و این عمل کاملا تصادفی انجام می شود. در بیشتر حالات باج افزار از RSSA-1024 به عنوان کلید استفاده می کند. مشاهده ی نوع جدیدی از باج افزارها که از ۱۰ کلید متفاوت استفاده می کند قابل توجه می باشد.

توسعه دهندگان باج افزارها همچنان در حال کشف آپشن های جدید برای خطرناک تر کردن محصولاتشان هستند. کم شدن شانس قربانیان در بازگردانی فایل ها باعث افزایش درآمد قربانیان از این باج افزارها خواهد شد. تا این لحظه همچنان مشخص نیست که به حمله کنندگان پشت Azer باید پرداخت نمود تا از شر این بدافزار خلاص شد. این بدافزار آخرین نسخه از CryptoMix نبود و همچنین خلافکاران پشت این بدافزار حتما آن را بهبود خواهند بخشید.

گردآورنده: محمد مرتضوی

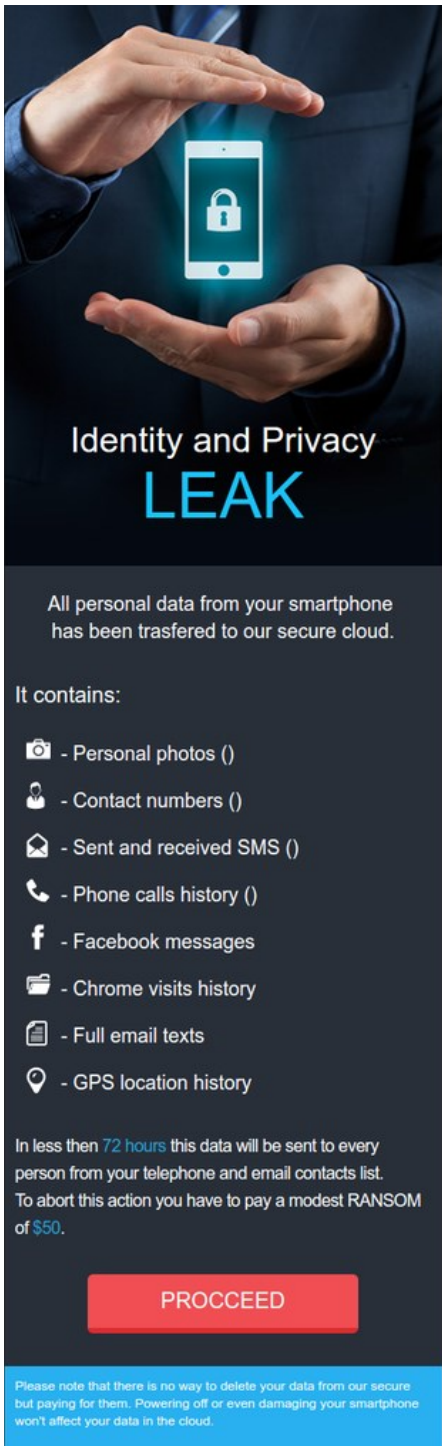
اندروید هم در امان نیست! باج افزار LeakerLock

یک نوع جدید از باج افزار اندروید در Google Play کشف شده است که قربانیان را تهدید می کند که اطلاعات شخصی آنان و تاریخچه ی جستجوی آنان در اینترنت را با دیگر اعضای مخاطبینی که در گوشی فرد موجود است به اشتراک می گذارد.

این باج افزار توسط محققان امنیتی McAfee کشف شده است. این باج افزار در اصل اطلاعات شما را رمزنگاری نمی کند اما در عوض به جای اینکار، یک نسخه ی پشتیبان از داده های ذخیره شده برروی وسیله ی مورد نظر را نزد خود نگه می دارد و قربانی را تهدید می کند که در ازای پخش نکردن این اطلاعات با سایر مخاطبین باید مبلغی را بپردازد.

افراد پشت این باج افزار مبلغ ۵۰ دلار را در ازای پخش نکردن اطلاعاتی همچون تصاویر، پیغام های فیس بوک، تاریخچه ی مرورگر، ایمیل ها، لوکیشن و غیره از قربانی تقاضا می کنند.دو اپلیکیشنی که در Google Play شامل این بدافزار بودند.Wallpapers Blur HD، نام یکی از این اپلیکیشن ها می باشد که بین ۵۰۰۰ تا ۱۰۰۰۰ بار دانلود شده است. همچنین Booster & Cleaner Pro یکی دیگر از این برنامه ها می باشد که بین ۱۰۰۰ تا ۵۰۰۰ دفعه دانلود شده است.

مجموع این اعداد نشان می دهد که میانگین ۱۵۰۰۰ نفر قربانی این باج افزار شده اند. این بدافزارها از ماه آپریل در Google Play قرار دارند. هردوی این اپلیکیشن ها امتیاز



بالایی را نیز در Google Play داشتند که تمامی نظرات در پشت این طرح، بررسی هایی تقلبی بودند.

به محض اینکه شما LeakerLocker را دانلود می کنید، از شما دسترسی های فراوانی را اپلیکیشن می خواهد. این دسترسی ها شامل مدیریت تماس ها، خواندن و ارسال پیامک و دسترسی به مخاطبین می باشد.

این مفهوم درست است که بدافزار توانایی جمع آوری اطلاعات شخصی را دارد اما تمامی اطلاعات شخصی قابل دسترسی و یا نشر نمی باشد.

بنابراین آنالیز کدها نشان می دهد که این بدافزار قابلیت دسترسی به آدرس ایمیل ها، برخی از اطلاعات مخاطبین، تاریخچه ی مرورگر کروم، پیام های متنی، تماس ها و تصاویر از دوربین را دارا می باشد.

قطعات داده به صورت تصادفی انتخاب می شود تا قربانی متقاعد که تمامی دادهایش کپی شده است. اگرچه در این لحظه اطلاعات قربانی در حقیقت کپی نشده است. اما این امر اگر سرور کنترل دستورالعمل های مربوطه را ارسال نماید ممکن است اتفاق افتد.

فرم مربوط به این باج افزار میزان باج را از کاربر با استفاده از کارت های اعتباری تقاضا می کند. محققان به قربانیان توصیه می کنند تا پرداختی انجام ندهند، زیرا هیچ تضمینی برای انتشار اطلاعات وجود ندارد.

محققان McAfee این باج افزار را (LeakerLocker) به گوگل گزارش کرده اند که گفته می شود با بررسی ها مشخص شد که دو اپلیکیشن از Google Play حذف شدند.

گردآورنده: محمد مرتضوی

نسخه ی Exte از باج افزار CryptoMix

Rivero محقق باج افزاری MalwareByte نوع جدیدی از باج افزار CryptoMix را کشف کرده است که فایل های رمزنگاری شده را با پسوند .EXTE ذخیره می کند. در این مقاله به صورت خلاصه به این باج افزار پرداخته خواهد شد.

عملیات رمزنگاری همانند ورژن قبلی در این باج افزار انجام می شود ولی چندین تفاوت موجود است. در ابتدا توضیحات باج افزار تغییر کرده و در فایلی به نام _HELP_INSTRUCTION.TXT قرار دارد. توضحیات این باج افزار شامل راهنمایی هایی در خصوص ارتباط با آدرس های زیر برای پرداخت می باشد.

exte1@msgden.net، exte2@protonmail.com و یا exte3@reddithub.com

تغییر قابل توجه دیگر فرمت فایل های رمزنگاری شده می باشد. در این ورژن زمانی که یک فایل توسط باج افزار رمزنگاری می شود، فرمت .EXTE به آن تعلق می گیرد. برای مثال یک فایل که به صورت امتحانی توسط این باج افزار رمزنگاری شد، نام آن به

32A1CD301F2322B032AA8C8 625EC0768.EXTE تغییر یافت.

یک نکته ی جالب این می باشد که این نسخه از باج افزار نیز همچنان از ۱۰ کلید عمومی RSA همانند ورژن قبلی خود یعنی Azer استفاده می کند. یکی از این کلیدها به صورت تصادفی برای رمزنگاری فایل های کاربرانتخاب می شود. این ویژگی به باج افزار اجازه می دهد تا به صورت Offlineبه راحتی به کار خود ادامه دهد.

در ادامه آنالیزهایی از این باج افزار آمده است.

File Hashes:

SHA256: 6211fdd680208f94aa0149619fac-c0de8b51e6cb98108132d539469f3affa712

نام فایل ها در نسخه ی Exte

_HELP_INSTRUCTION.TXT

%AppData%\[random].exe

متن باج افزار:

Hello!

Attention! All Your data was encrypted!

For specific informartion, please send us an email with Your ID number:

exte1@msgden.net

exte2@protonmail.com

exte3@reddithub.com

We will help You as soon as possible!

DECRYPT-ID-[victim_id] number

ایمیل های مربوط به باج افزار:

exte1@msgden.net

exte2@protonmail.com

exte3@reddithub.com

گردآورنده: محمد مرتضوی

باج افزار Reyptson

محققان xXToffeeXx شرکت امنیتی Emsisoft باج افزار جدیدی با نام Reyptson یافتند که اسپانیایی ها را مورد هدف خود قرار می دهد. همچنین، فعالیت های رو به افزایشی در توسعه ی این باج افزار مشاهده گردیده است. محققان امنیتی MalwareHunterTeam امروز نگاهی عمیق تر به این باج افزار و توزیع مستقیم اسپم از قربانیان توسط ایمیل خواهند داشت.

این ویژگی بسیار جدید است و در هیچ یک از باج افزارهای قبلی مشاهده نگردیده است. بنابراین تصمیم گرفتیم تا با نگاهی عمیق‌تر به موضوع ببینیم که از آن چه مواردی را می توان متوجه شد.

باج افزار Reyptson با اسپم مخاطبین Thunderbird قربانی، خودش را گسترش می دهد.

برخلاف باقی باج افزار ها که به خاطر داریم، Reyptson قابلیت گسترش خود را از طریق ارسال ایمیل اسپم از کامپیوتر قربانی دارد. این باج افزار با بررسی نصب بودن سرویس ایمیل Thunderbird، سعی به خواندن لیست مخاطبین قربانی می کند.

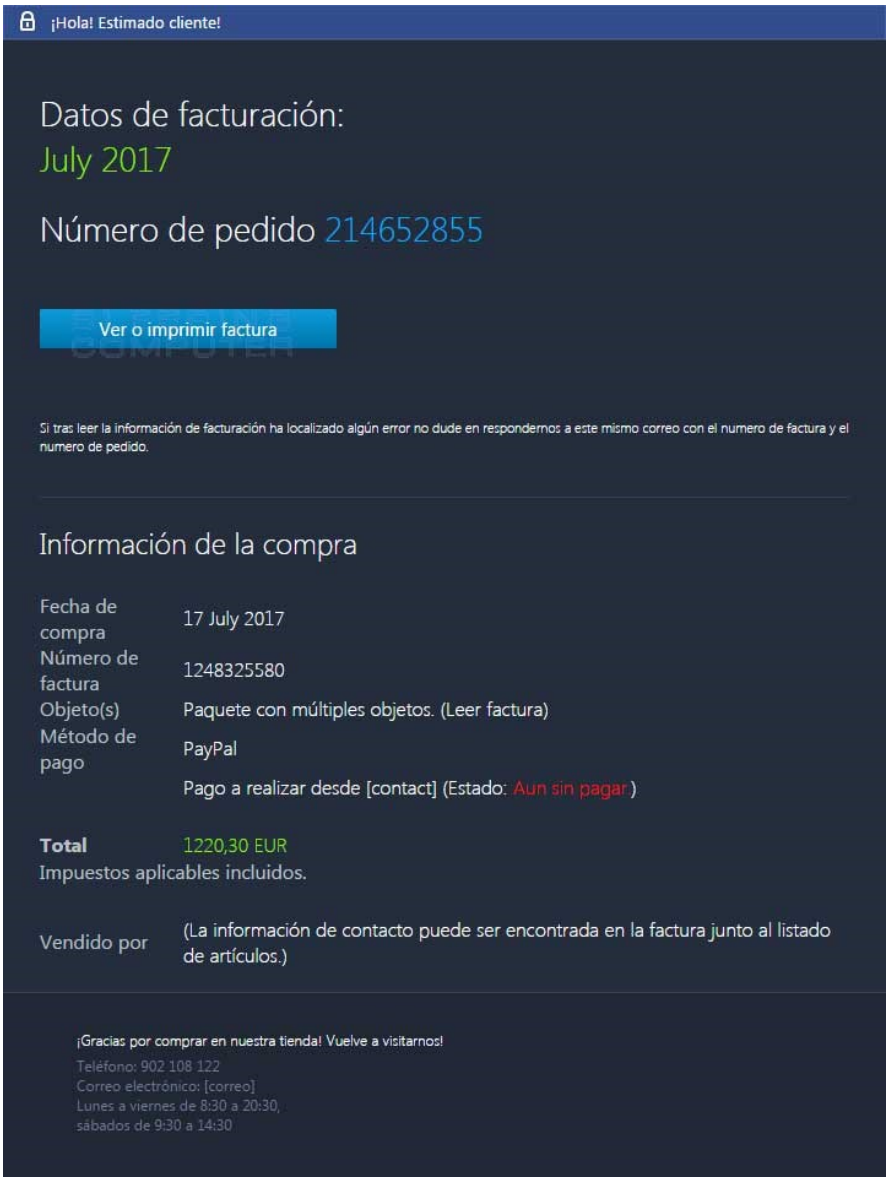
اگر این باج افزار توانایی خواندن و اجازه ی دسترسی به لیست مخاطبین را پیدا کند، شروع به ارسال ایمیل اسپم برای مخاطبین قربانی می کند.

موضوع ایمیل های ارسالی Folcan S.L. Facturación می باشد که شامل اطلاعات مربوط به صورتحساب های جعلی می باشد. متن اصلی این ایمیل به زبان اسپانیایی است و از کاربر خواسته می شود تا برروی لینکی از این صورتحساب ها کلیک نماید. زمانی که گیرنده برروی این لینک کلیک نماید، فایلی به نام factura.pdf.rar که شامل یک فایل اجرایی است دانلود می گردد. این فایل اجرایی کاربر را به محض باز کردن، به بد افزار نام برده آلوده می کند.

باج افزار Reyptsonچگونه کامپیوترها را کدگذاری می کند؟

زمانی که کاربر فایل اجرایی دانلود شده را باز نماید، یک فایل صورتحساب در قالب PDF نمایش داده می شود.

ادامه در صفحه ی بعد.



گردآورنده: محمد مرتضوی

باج افزار Reyptson (ادامه...)

به محض باز شدن، باج افزار به سرور کنترل و فرمان وصل شده و یک شناسه ی یکتا را برای سرور ارسال می کند. این شناسه شامل سریال سیستم، یک نام کاربری و زمان حال حاضر به میلی ثانیه می باشد.

زمانی که این شناسه ارسال شد یک کوکی با نام UJBTFity و مقدار KuyfibvUYFOUygonULIHLuhg oYUHGV در کامپیوتر کاربر ایجاد و برای سرور ارسال می شود. هنوز مشخص نیست که این کوکی برای چه عملی ایجاد می شود اما ممکن است به عنوان یک شناسه ی وابسته به پیاده سازی RaaS باشد.

سرور برای کاربر یک رشته ی کدگذاری، نام کاربری و رمز عبور ارسال می کند که کاربر می تواند با آن وارد سیستم پرداخت شود.

زمانی که رشته ی فوق از سوی سرور ارسال گردد، فایل های کامپیوتر قربانی که دارای فرمت زیر هستند، رمزنگاری می شوند.

.doc, .dot, .wbk, .docx, .docm, .dotx, .dotm, .docb, .xls, .xlt, .xlm, .xlsx, .xlsm, .xltx, .xltm, .xlsb, .xla, .xlam, .xll, .xlw, .ppt, .pot, .pps, .pptx, .pptm, .potx, .potm, .ppam, .ppsx, .ppsm, .sldx, .sldm, .accdb, .db, .accde, .accdt, .accdr, .pdf, .ani, .anim, .apng, .art, .bmp, .bpg, .bsave, .cal, .cin, .cpc, .cpt, .dds, .dpx, .ecw, .exr, .fits, .flic, .flif, .fpx, .gif, .hdri, .hevc, .icer, .icns, .ico, .cur, .ics, .ilbm, .jbig, .jbig2, .jng, .jpeg, .jpeg, .2000, .jpeg-ls, .jpeg, .xr, .kra, .mng, .miff, .nrrd, .ora, .pam, .pbm, .pgm, .ppm, .pnm, .pcx, .pgf, .pictor, .png, .psd, .psb, .psp, .qtvr, .ras, .rbe, .jpeg-hdr, .logluv, .tiff, .sgi, .tga, .tiff, .tiff, .ufo, .ufp, .wbmp, .webp, .xbm, .xcf, .xpm, .xwd, .cpp, .h, .cs, .sln, .idb, .txt, .dat

اگر باج افزار به هریک از فایل ها با فرمت مطرح شده که در پوشه های زیر نباشد، مواجه شود، عملیات رمزنگاری شروع می شود.

c:\windows, c:\windows.old, c:\users\default, c:\users\all users, c:\users\public, c:\program files, c:\$recycle.bin, c:\program files (x86), c:\programdata, c:\system volume information, %UserProfile%\appdata

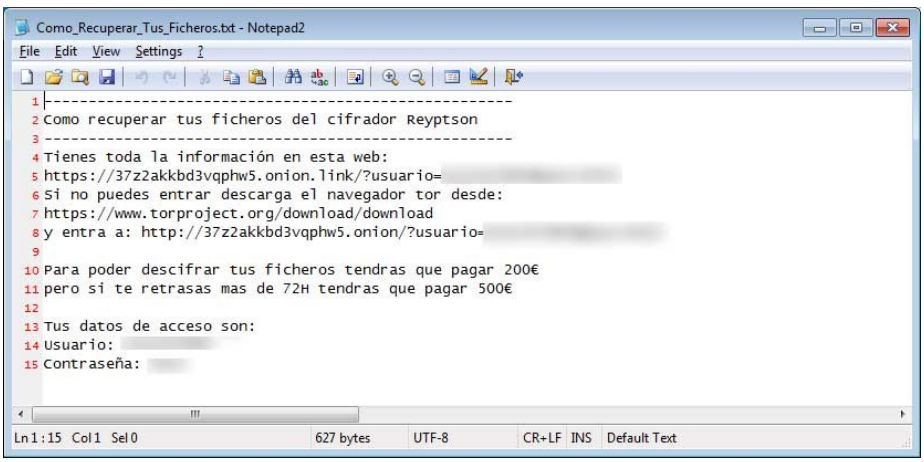
زمانی که رمزنگاری فایل ها تمام شد، فرمت Reyptson به انتهای آنان اضافه می شود.

همچنین این باج افزار یک فایل حاوی اطلاعات پرداخت و توضیحات با نام Como_Recuperar_Tus_Ficheros.txt در هر پوشه ایجاد می کند.

همچنین بعد از این عملیات، این باج افزار یک فایل PDF تقلبی را باز می کند تا PDF Reader پیغامی مبنی بر نامعتبر بودن را نمایش دهد. با این کار قربانی بیشتر متقاعد می شود که یک فایل PDF رمزنگاری شده باز شده است.

بعد از آن فایل %AppData%\Spotify\SpotifyWebHelper\SpotifyWebHelper.exe اجرا شده و توضیحات اضافه ای شامل اطلاعاتی مربوط به نحوه دسترسی به سرویس پرداخت نمایش داده می شود.

ادامه در صفحه ی بعد.

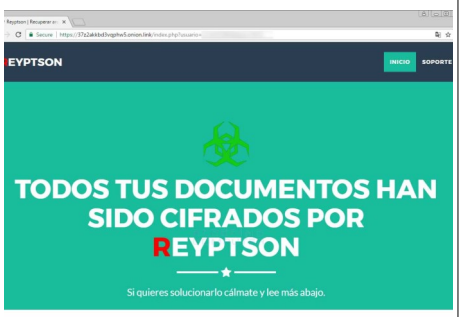


گردآورنده: محمد مرتضوی

باج افزار Reyptson (ادامه...)

سرور پرداخت باج افزار

توضیحات باج افزار دارای لینکی به سرور پرداخت در شبکه ی Tor می باشد که کاربر با ورود به آن می تواند راهنمایی های مربوط به پرداخت را مشاهده کند. میزان مبلغ درخواستی در ابتدا ۲۰۰ یورو می باشدکه پس از ۷۲ ساعت به ۵۰۰ یورو می رسد. درخواست مبلغی از قربانی در واحدی به غیر از بیت کوین یک حرکت تازه ای است که کمی باعث سردرگمی کاربران شده است.



در ادامه اطلاعات مختصری از این باج افزار آورده شده است.

IOC

Hashes:

SHA256: e6d549543863cd3eb7d92436739a66da4b2cc1a9d40267c4bb2b2fa50bf42f41

Network Communication:

http://www.melvinmusicals.com/facefiles/

http://37z2akkbd3vqphw5.onion/?usuario=[user_id]&pass=[password]

http://37z2akkbd3vqphw5.onion.link/?usuario=[user_id]&pass=[password]

Files associated with the Reyptson Ransomware:

%AppData%\Spotify\

%AppData%\Spotify\SpotifyWebHelper\

%AppData%\Spotify\SpotifyWebHelper\dat

%AppData%\Spotify\SpotifyWebHelper\fin

%AppData%\Spotify\SpotifyWebHelper\Reyptson.pdf

%AppData%\Spotify\SpotifyWebHelper\Spotify.vbs

%AppData%\Spotify\SpotifyWebHelper\SpotifyWebHelper.exe

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