باج افزارها

تهیه شده توسط گروه لیان

liangroup

9100 41 51
@liansec
lian_gpco
www.liangroup.net

چگونه از شبکه
خود در برابر
باج افزارها
محافظت کنیم

محافظت از شبکه در برابر باج افزارها

RANSOMWARE

باج افزارها در حال حاضر سریع‌ترین تهدید بدافزاری محسوب می‌شوند که انواع مختلف کاربران؛ از کاربر خانگی گرفته تا شبکه‌های شرکتی را هدف قرار می‌دهند. به طور متوسط، از اول ژانویه ۲۰۱۶ بیش از ۴۰۰۰ حمله باج افزار به‌صورت روزانه رخ داده است. این نشان دهنده‌ی افزایش ۳۰۰ درصدی نسبت به سال ۲۰۱۵ است که متوسط این حملات حدود ۱۰۰۰ حمله در روز بود. پیشگیری‌ها و اقدامات بسیار موثری وجود دارد که می‌توانند خطر ایجاد شده را به میزان قابل توجهی کاهش دهند. باج افزارها کاربران خانگی، مشاغل و شبکه‌های دولتی را هدف قرار می‌دهند و می‌توانند منجر به از دست دادن موقتی یا دائمی اطلاعات حساس یا انحصاری، ایجاد اختلال در عملکرد منظم، خسارت‌های مالی جهت بازیابی سیستم‌ها و فایل‌ها و همچنین آسیب احتمالی به اعتبار یک سازمان شوند. باج افزار ممکن است یک کاربر را به سوی کلیک روی لینک پرداخت یک باج افزار هدایت کند. اگرچه، ممکن است این لینک، لینکی مخرب باشد و منجربه واگیری‌های مخرب بیشتری شود. برخی از انواع باج افزار، پیام‌های ترسناکی را نمایش می‌دهند، پیام‌هایی از قبیل: «رایانه شما جهت بازدید از وب سایت‌هایی با محتوای غیرقانونی استفاده شده است. برای باز کردن قفل کامپیوتر، باید ۱۰۰ دلار جریمه پرداخت کنید.» «شما فقط ۹۶ ساعت فرصت دارید تا مبلغ موردنظر ما را پرداخت کنید. اگر در زمان تعیین شده پول را واریز نکنید، تمامی فایل‌های شما برای همیشه رمزگذاری می‌شوند و هیچ کس نمی‌تواند آن‌ها را بازیابی کند.»

RANSOMWARE

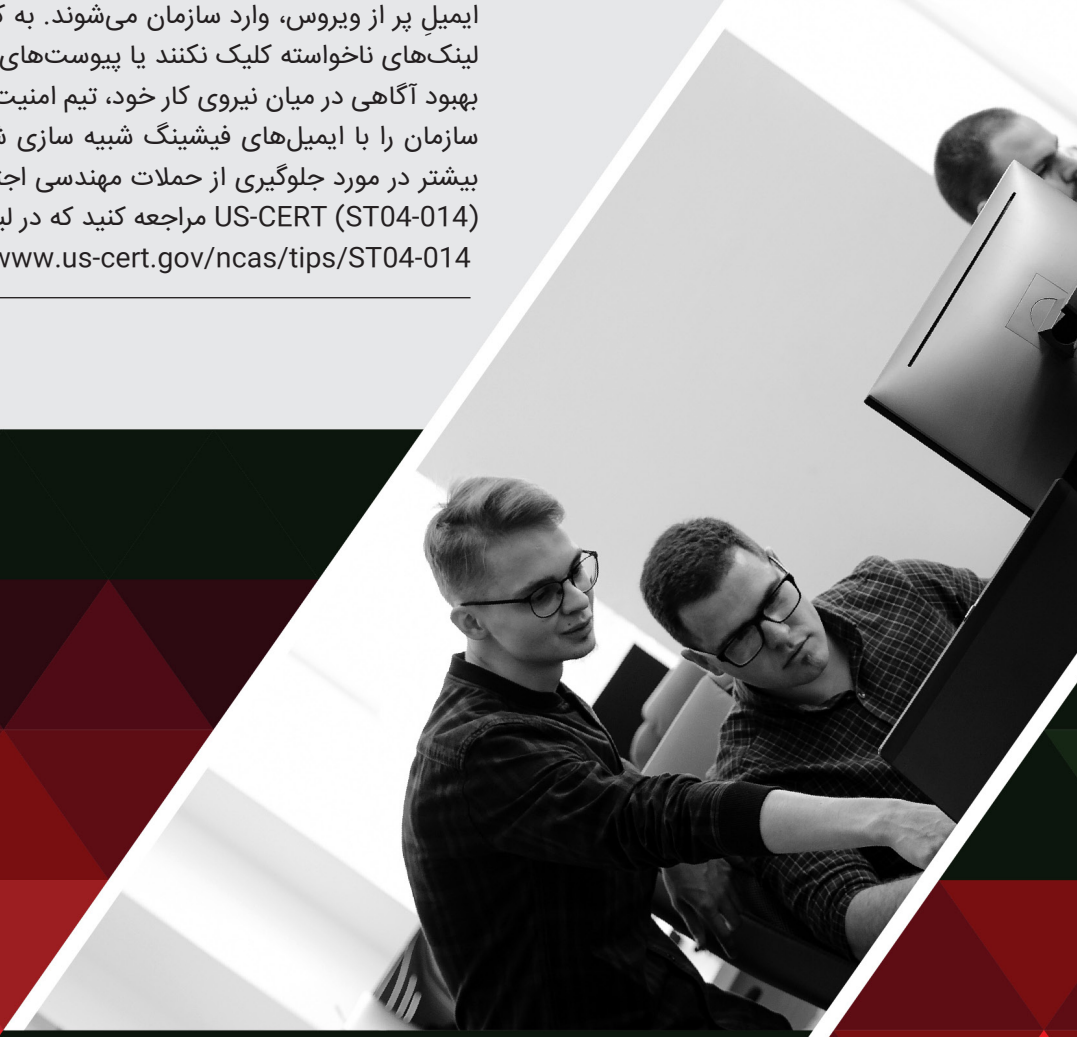
باج افزار چیست؟

باج افزار، نوعی بدافزار است که داده‌ها و سیستم‌های مهم شما را با هدف اخاذی مورد هدف قرار می‌دهد. باج افزار به طور مکرر از طریق ایمیل‌های spearphishing (کلاهبرداری از طریق سد راه کردن) تحویل داده می‌شود. پس از اینکه دسترسی کاربر از داده‌ها یا سیستم برداشته شد، هکر خواستار پرداخت پول برای این باج افزار می‌شود. پس از دریافت هزینه، هکر راهی برای دسترسی مجدد به سیستم یا داده‌ها در اختیار قربانی قرار می‌دهد. تکرارهای پیشین این فرایند نشان می‌دهد که سازمان‌ها و اندیوزرها نیز در تله‌ی باج‌افزارها افتاده‌اند و این موضوع آگاهی و آموزش را به عنوان یک اقدام پیشگیرانه به امری حیاتی تبدیل کرده است.

محافظت از شبکه‌های خود

به کارمندان خود آموزش دهید

مهاجمان اغلب با فریب کاربر جهت فاش‌کردن رمز عبور یا با کلیک روی پیوست یک ایمیلِ پر از ویروس، وارد سازمان می‌شوند. به کارکنان خود یادآوری کنید که هرگز روی لینک‌های ناخواسته کلیک نکنند یا پیوست‌های ناخواسته را در ایمیل‌ها باز نکنند. برای بهبود آگاهی در میان نیروی کار خود، تیم امنیت داخلی می‌تواند آموزش نیروی کار یک سازمان را با ایمیل‌های فیشینگ شبیه سازی شده آزمایش کند. برای کسب اطلاعات بیشتر در مورد جلوگیری از حملات مهندسی اجتماعی و فیشینگ، لطفاً به نکته امنیتی US-CERT (ST04-014) مراجعه کنید که در لینک زیر، قابل دسترسی است:
https://www.us-cert.gov/ncas/tips/ST04-014



پیشگیری فعالانه بهترین دفاع است

پیشگیری موثرترین دفاع در برابر باج افزارها است و همچنین اتخاذ اقدامات احتیاطی برای محافظت، امری حیاتی است. واگیری‌ها می‌توانند برای یک فرد یا سازمان ویرانگر باشند و بهبودی از این امر می‌تواند فرآیند دشواری باشد که نیازمند به‌کارگیری یک متخصص معتبر بازیابی اطلاعات می‌باشد. دولت ایالات متحده (USG) به کاربران و ادمین‌ها توصیه می‌کند اقدامات پیشگیرانه زیر را برای محافظت از شبکه‌های رایانه‌ای خود، به‌منظور جلوگیری از ابتلا به فراگیرشدن باج افزار انجام دهند:

اقدامات پیشگیرانه

- یک برنامه آموزشی جهت آگاهی و تمرین، پیاده سازی کنید. از آنجا که اندیوزرها هدف هستند، کارکنان و افراد باید از تهدید باج افزارها و نحوه‌ی در دام افتادن، آگاه باشند.
- فیلترهای اسپم قوی را جهت جلوگیری از دسترسی ایمیل‌های فیشینگ به اندیوزرها و تأیید اعتبار ایمیل ورودی با استفاده از فناوری‌هایی مانند Sender Policy Framework (SPF)، گزارش و مطابقت اعتبار سنجی پیام دامنه (DMARC) و نامه شناسایی شده DomainKeys (DKIM) را فعال کنید؛ تا از کلاهبرداری ایمیلی جلوگیری کرده باشید.
- تمام ایمیل‌های ورودی و خروجی را اسکن کنید تا تهدیدات را شناسایی کرده و فایل‌های اجرایی را از رسیدن به دست کاربران نهایی (اندیوزر ها) فیلتر کنید.
- فایروال‌ها را برای جلوگیری از دسترسی به آدرس‌های IP مخرب شناخته‌شده، پیکربندی کنید.
- سیستم عامل‌ها، نرم افزار و firmware را روی دستگاه‌ها Patch کنید. استفاده از یک سیستم مدیریت Patchمتمرکز را در نظر داشته باشید.
- برنامه‌های ضد ویروس و ضد بدافزار را تنظیم کنید تا اسکن منظم را به طور خودکار انجام دهد.
- مدیریت استفاده از حساب‌های امتیازمحور براساس اصل حداقل امتیاز: به هیچ کاربری نباید دسترسی اداری اختصاصی داده شود مگر اینکه کاملاً ضروری باشد. و کسانی که به حساب‌های اصلی (ادمین) نیاز دارند فقط در صورت لزوم باید از آن‌ها استفاده کنند.
- کنترل‌های دسترسی، از قبیل مجوزهای اشتراک فایل، فهرست و شبکه را با کمترین امتیاز در نظر داشته باشید. اگر کاربری فقط نیاز دارد که فایل‌های خاصی را «بخواند»، نباید دسترسی نوشتاری به آن فایل‌ها، دایرکتوری‌ها یا اشتراک‌ها داشته باشد.
- اسکریپت‌های ماکرو را از فایل‌های آفیس (که از طریق ایمیل منتقل می‌شوند) غیرفعال کنید. برای باز کردن فایل‌های Microsoft Office که از طریق ایمیل منتقل شده‌اند، از نرم افزار Office Viewer به جای برنامه‌های کامل مجموعه آفیس، استفاده کنید.
- سیاست‌های محدودیت نرم افزار (SRP) یا سایر کنترل‌ها را جهت جلوگیری از اجرای برنامه‌ها، از مکان‌های رایج باج افزار، مانند پوشه‌های موقت پشتیبانی‌کننده از مرورگرهای معروف اینترنت یا برنامه‌های فشرده/ غیرفشرده‌سازی، از جمله پوشه AppData / Loca-lAppData پیاده سازی کنید.
- در صورت عدم استفاده از پروتکل RDP (Remote Desktop)، آن را غیرفعال کنید.
- از «لیست سفید» برنامه استفاده کنید، که به سیستم‌ها اجازه می‌دهد فقط برنامه‌های شناخته‌شده و مجاز توسط سیاست‌های امنیتی را اجرا کند.
- محیط‌های سیستم عامل یا برنامه‌های خاص را در یک محیط مجازی اجرا کنید.
- طبقه بندی داده‌ها بر اساس ارزش سازمانی و پیاده‌سازی تفکیک فیزیکی و منطقی شبکه‌ها و داده‌ها برای واحدهای مختلف سازمانی.

ملاحظات تداوم کسب‌وکار

- به طور منظم از داده‌ها نسخه پشتیبان (بکاپ) تهیه کنید. صحت آن نسخه پشتیبان را تأیید کنید و روند بازیابی را برای اطمینان از عملکرد آن آزمایش کنید.
- به‌صورت سالانه تست نفوذ و ارزیابی آسیب پذیری را انجام دهید.
- پشتیبان‌هایی که گرفته‌اید را ایمن کنید. اطمینان حاصل کنید که نسخه‌های پشتیبان به طور دائم به رایانه‌ها و شبکه‌هایی که این پشتیبان از آن‌ها گرفته شد، متصل نیستند. برای مثال می‌توان به ایمن سازی نسخه پشتیبان در فضای ابری یا ذخیره فیزیکی نسخه پشتیبان به‌صورت آفلاین اشاره کرد. برخی از موارد باج افزار می‌توانند پشتیبان‌گیری ابری در هنگام پشتیبان گیری مداوم سیستم به‌صورت همزمان را، قفل کنند. این امر همچنین به عنوان همگام سازی مداوم نیز شناخته می‌شود. پشتیبان گیری، در بازیابی و پاسخ باج افزار بسیار مهم است. اگر آلوده باشید، تهیه نسخه پشتیبان ممکن است بهترین راه برای بازیابی اطلاعات مهم شما باشد.

در صورت آلوده‌شدن به باج افزار چه کاری باید انجام دهید

دولت ایالات متحده توصیه می‌کند که در صورت عدم موفقیت اقدامات پیشگیرانه، سازمان‌ها اقدامات زیر را به‌هنگام آلوده شدن به باج افزار انجام دهند:

- بلافاصله رایانه آلوده را ایزوله (جدا) کنید. سیستم‌های آلوده باید در اسرع وقت از شبکه خارج شوند تا از حمله باج افزار به شبکه یا درایوهای به اشتراک گذاشته‌شده، جلوگیری شود.
- دستگاه‌های آلوده‌شده‌ای که هنوز کاملاً خراب نشده‌اند، جدا یا خاموش کنید. این امر ممکن است زمان بیشتری را برای پاکسازی و بازیابی داده‌ها، حفظ آسیب دیدگی و جلوگیری از بدترشدن شرایط فراهم کند.
- با استفاده از آفلاین کردن سیستم‌ها و یا اطلاعات پشتیبان، آن‌ها را بلافاصله ایمن کنید. اطمینان حاصل کنید که پشتیبان‌گیری فاقد بدافزارها است.
- بلافاصله با پلیس تماس بگیرید. در صورت گزارش مشاهده یک باج افزار، شدیداً به شما توصیه می‌کنیم که بلافاصله پس از کشف، درخواست کمک داده و با یک دفتر محلی اداره تحقیقات فدرال (FBI) یا سرویس مخفی ایالات متحده تماس بگیرید.
- در صورت دسترسی، بخش‌های جزئی از داده‌های موجود که توسط باج افزار مورد حمله واقع‌شده را جمع آوری و ایمن کنید.
- در صورت امکان، پس از حذف سیستم از شبکه، کلمه عبور حساب‌های آنلاین و رمزهای عبور شبکه را تغییر دهید. همچنین، پس از حذف بدافزار از سیستم، همه رمزهای عبور سیستم را تغییر دهید.
- مقادیر و فایل‌های رجیستری را حذف کنید تا بارگیری برنامه متوقف شود.

برنامه‌ی پاسخگویی به حوادث امنیتی و تداوم تجارت خود را اجرا کنید. در حالت ایده‌آل، سازمان‌ها اطمینان حاصل می‌کنند که از پشتیبان گیری مناسبی برخوردار هستند. در نتیجه پاسخ آن‌ها در مواجهه با یک حمله، بسیار ساده است و داده‌ی مورد نظر از یک پشتیبان عاری از بدافزار و شناسایی شده، تهیه می‌کنند. داشتن پشتیبان از اطلاعات می‌تواند شما را از پرداخت پول به باج افزار (جهت بازیابی اطلاعات) بی‌نیاز کند.

خطرات جدی وجود دارند که باید پیش از پرداخت پول به باج افزار، آن‌ها در نظر بگیرید. دولت، پرداخت پول به عاملان تهداد را توصیه نمی‌کند. با این وجود، پس از به خطر افتادن سیستم‌ها، پرداخت پول یک تصمیم جدی است که نیاز به ارزیابی همه‌ی گزینه‌ها جهت محافظت از سهامداران، کارکنان و مشتریان است. قربانیان ممکن است بخواهند امکان فنی، به موقع و هزینه راه اندازی مجدد سیستم‌ها را به‌کمک نسخه پشتیبان؛ ارزیابی کنند. این قربانیان همچنین ممکن است بخواهند عوامل زیر را در نظر بگیرند:

- پرداخت پول، تضمینی برای دسترسی مجدد سازمان به داده‌هایشان ندارد. در حقیقت، برخی از افراد یا سازمان‌ها پس از پرداخت پول هرگز کلیدی برای رمزگشایی فایل‌های قفل شده دریافت نکردند.
- برخی از قربانیانی که تقاضای باج افزار را پرداخت کردند، دوباره توسط عاملان تهدید سایبری هدف قرار گرفتند.
- پس از پرداخت پولی که از قربانی خواسته شده، از برخی از قربانیان درخواست می‌شود که برای دریافت کلید رمزگشایی هزینه بیشتری بپردازند.
- پرداخت پول می‌تواند این مدل تجارت جنایی را به‌صورت سهوی تشویق کند.

چگونه اقدام قانونی می‌تواند کمک کند

هر سیستمی که آلوده به باج افزار شود، اولین قدم این است که باید فوراً با پلیس تماس بگیرید. اقدام قانونی ممکن است بتواند از مراجع قانونی و ابزارهایی استفاده کند که در دسترس اکثر سازمان‌ها نیست. اقدام قانونی همچنین می‌تواند از شرکای اجرای قانون بین المللی جهت یافتن اطلاعات به سرقت رفته یا رمزگذاری شده یا شناسایی مجرم، کمک بگیرد. این ابزارها و روابط می‌توانند احتمال دستگیری موفقیت آمیز مجرم را تا حد زیادی افزایش دهند و از این طریق، از ضررهای بعدی جلوگیری کنند. اجرای قانون دولتی، انجام تحقیقات سایبری را اولویت قرار می‌دهد؛ به گونه‌ای که باعث اختلال جزئی در عملکرد عادی یک بخش قربانی باج افزار می‌شود و به دنبال همکاری خاص با آن بخش است. اجرای قانون دولتی از اقدامات تحقیقاتی‌ای استفاده می‌کند که از توقف غیرضروری یا جابجایی کارکنان یک شرکت جلوگیری می‌کند. اقدامات قانونی، فعالیت‌هایش را از نزدیک با سازمان آسیب‌دیده هماهنگ می‌کند، تا از افشای ناخواسته اطلاعات جلوگیری کند. همزمان با بهبودی یک نهاد آسیب‌دیده از یک حادثه امنیت سایبری، نهاد مذکور باید اقدامات لازم جهت جلوگیری از حوادث مشابه را آغاز کند. آژانس‌های اجرای قوانین و مراکز امنیت ملی می‌توانند به سازمان‌ها در اجرای اقدامات متقابل کمک کرده و اطلاعات و بهترین روش‌ها (Best Practice) را جهت پیشگیری از حوادثی از این دست در آینده ارائه دهند. علاوه بر این، سازمان متضرر باید بازبینی پس از حادثه را در مورد پاسخ خود به حادثه انجام دهد و نقاط قوت و ضعف برنامه پاسخگویی به حادثه را ارزیابی کند. (ارزیابی عملکرد)

انواع (نسخه‌های مختلف) باج افزار

باج افزار یک فعالیت جنایی در حال رشد است که شامل نسخه‌ها و انواع مختلفی است. از سال 2012 که نسخه‌های مختلف باج افزار لاکر معرفی شد، نسخه‌های باج افزار پیچیده‌تر و مخرب‌تر شده‌اند. برخی از انواع آن‌ها نه تنها فایل‌های موجود در دستگاه آلوده را رمزگذاری می‌کنند، بلکه محتویات درایوهای مشترک یا شبکه‌ای، دستگاه‌های رسانه‌ای ذخیره سازی که به‌صورت خارجی متصل می‌شوند و همچنین سرویس‌های ذخیره سازی ابری را که به رایانه‌های آلوده متصل هستند، را نیز رمزگذاری می‌کنند. از آنجا که این نسخه‌های باج افزار فایل‌های کاربران و سازمان‌ها را رمزگذاری کرده و تا زمان پرداخت پول، این فایل‌ها را بلااستفاده می‌کنند، باج افزارهای مخرب تلقی می‌شوند.

تحقیقات اخیر فدرال توسط FBI نشان می‌دهد که نویسندگان باج افزار همچنان با استفاده از سرویس‌های ناشناس مانند «Tor» ، برای برقراری ارتباط بین سیستم‌های آلوده و ارز مجازی بیت کوین برای جمع آوری باج‌ها، کد باج افزار را بهبود می‌بخشند.

Tor 3 نرم افزاری رایگان برای امکان برقراری ارتباط ناشناس است. Tor با استفاده از یک شبکه داوطلبانه رایگان، جهانی و متشکل از بیش از 7000 رله، ترافیک اینترنت را جهت پنهان کردن مکان و کاربرد کاربر از هر کسی که نظارت شبکه یا تجزیه و تحلیل ترافیک را انجام می‌دهد، هدایت می‌کند. (این نام از نام اصلی پروژه نرم افزار، The Onion Router گرفته شده است.)

در حال حاضر، پنج گزینه برتر باج افزار که شرکت‌ها و افراد مختلفی را در ایالات متحده هدف قرار داده است، MSIL / Samas، TeslaCrypt، CTBLocker، CryptoWall و Locky هستند. نسخه‌های جدید باج افزار به طور مداوم در حال ظهور هستند.

CryptoWall

CryptoWall و انواع آن از آوریل ۲۰۱۴ به طور فعال برای هدف قرار دادن قربانیان ایالات متحده مورد استفاده قرار گرفته است. CryptoWall اولین نوع باج افزار بود که پرداخت پول را فقط به‌صورت بیت کوین می‌پذیرفت. مقادیر باج‌های مربوط به CryptoWall معمولاً بین ۲۰۰ تا ۱۰،۰۰۰ دلار است. پس از حذف باتنتِ CryptoWall، CryptoLocker به موفق‌ترین نسخه باج افزار در مواجهه با قربانیان در سراسر جهان تبدیل شده است. بین آوریل ۲۰۱۴ تا ژوئن سال ۲۰۱۵، IC3 تعداد ۹۹۳ شکایت مربوط به CryptoWall دریافت کرده است، که خسارات قربانیان در مجموع بیش از ۱۸ میلیون دلار گزارش شده است.

این رقم شامل هزینه‌های اضافی متحمل شده توسط قربانی است. هزینه‌ها ممکن است با محدودیت‌های شبکه، اقدامات متقابل شبکه، از دست دادن بهره‌وری، هزینه‌های حقوقی، خدمات فناوری اطلاعات و خرید خدمات نظارت بر اعتبار برای کارمندان یا مشتریان نیز همراه باشد.

CryptoWall

CTB-Locker

CTB-Locker در ژوئن ۲۰۱۴ ظهور کرد و یکی از اولین نسخه‌های باج افزار است که از Tor برای زیرساخت C2 خود استفاده می‌کند. CTB-Locker به‌صورت انحصاری از Tor برای سرورهای C2 خود استفاده می‌کند و تنها پس از رمزگذاری فایل‌های قربانیان، به C2 متصل می‌شود. علاوه بر این، بر خلاف سایر انواع باج افزارها که از شبکه Tor برای برخی از ارتباطات استفاده می‌کنند، اجزای Tor در بدافزار CTBLocker تعبیه شده‌اند، که باعث می‌شود کارایی بیشتری داشته و تشخیص آن نیز دشوارتر شود. CTB-Lockerها همچنین از طریق بارگیری درایو و ایمیل‌های هرزنامه پخش می‌شود.

«Drive by download» انتقال نرم افزار مخرب به کامپیوتر قربانی بدون اطلاع و یا اقدام قربانی است.

« Malvertizing»، استفاده از تبلیغات مخرب در وب سایت‌های قانونی است. این تبلیغات مخرب حاوی کدی است که بدون هیچ گونه اقدامی از طرف کاربر، کاربر را آلوده می‌کند (یعنی کاربر برای آلوده شدن مجبور نیست روی تبلیغ کلیک کند)

CTB-Locker

TeslaCrypt

TeslaCrypt

TeslaCryptدر فوریه ۲۰۱۵ ظهور کرد و در ابتدا با رمزگذاری فایل‌های بازی، جامعه بازی‌های ویدیویی را هدف قرار داد. این فایل‌ها علاوه بر فایل‌هایی که معمولاً توسط باج افزار (اسناد، تصاویر و پرونده‌های پایگاه داده) هدف قرار می‌گرفتند، مورد حملات واقع شدند. پس از رمزگذاری داده‌ها، TeslaCrypt تلاش می‌کرد تا تمامی کپی‌هایShadow Volume و نقاط بازیابی سیستم را جهت جلوگیری از بازیابی مجدد فایل حذف کند. تسلا کریپت از طریق کیت‌های بهره‌برداری Sweet Orange، Angler و Nuclear توزیع شد.

Samas (SAMSAM) یا MSIL

Samas (SAMSAM) یا MSIL

MSIL یا Samas (SAMSAM) برای به خطر انداختن شبکه‌های قربانیان متعدد ایالات متحده، از جمله حملات ۲۰۱۶ به مراکز بهداشتی درمانی که نسخه‌های منسوخ‌شده برنامه مدیریت محتوای JBoss را اجرا می‌کردند، استفاده شد. SAMSAM از سرورهای آسیب‌پذیر مبتنی‌بر جاوا سوءاستفاده می‌کند. SAMSAM همچنین از ابزارهای منبع باز (Open Source) برای شناسایی و تدوین لیستی از میزبانانی که به فهرست فعال قربانی گزارش می‌دهند استفاده می‌کند. سپس عاملان تهدید از psexec.exe برای توزیع بدافزار به هر میزبان در شبکه و رمزگذاری بیشتر فایل‌های موجود در سیستم استفاده می‌کنند. عاملان تهدید برای ارائه‌ی کلیدهای رمزگشایی به قربانی، مقادیر مختلفی را به‌صورت بیت کوین دریافت می‌کنند.

Locky

Locky

در اوایل سال ۲۰۱۶، یک نوع ویرانگر باج افزار مخرب، Locky، رایانه‌های متعلق به مشاغل جهانی؛ از جمله در ایالات متحده، نیوزیلند، استرالیا، آلمان و انگلستان را آلوده کرد. لاکی از طریق ایمیل‌های هرزنامه که شامل اسناد مخرب مایکروسافت آفیس یا پیوست‌های فشرده‌شده (به عنوان مثال zip.، rar) است توزیع می‌شود که قبلاً با تروجان‌های بانکی مانند Dridex و Pony مرتبط بودند. پیوست‌های مخرب حاوی ماکرو یا فایل‌های JavaScript برای بارگیری پرونده‌های Locky هستند. اخیراً، این باج افزار با استفاده از کیت بهره‌برداری هسته‌ای نیز توزیع شده است.

Links to Other Types of Malware

سیستم‌های آلوده به باج افزار نیز اغلب به بدافزار دیگری آلوده می‌شوند. در مورد CryptoLocker، یک کاربر به طور معمول با باز کردن یک لینک مخرب از طریق ایمیل آلوده می‌شود. این لینک مخرب شامل Upatre (یک دانلود کننده) بود که کاربر را به GameOver Zeus آلوده کرد. GameOver Zeus گونه‌ای از تروجان‌های Zeus بود که برای سرقت اطلاعات بانکی و انواع دیگر داده‌ها مورد استفاده قرار می‌گرفت. پس از آلوده شدن سیستم به Upatre CryptoLocker، GameOver Zeus را نیز بارگیری می‌کند. سرانجام، CryptoLocker فایل‌ها را بر روی سیستم آلوده رمزگذاری می‌کرد و خواستار پرداخت هزینه می‌شد.
عملیات اختلال در برابر بات نت GameOver Zeus همچنین بر CryptoLocker نیز تأثیر گذاشت و این امر ارتباط نزدیک بین باج افزار و انواع دیگر بدافزارها را نشان می‌دهد. در ژوئن ۲۰۱۴، یک عملیات اجرای قانون بین المللی، با موفقیت زیرساخت‌های GameOverZeus و CryptoLocker را تضعیف کرد.