بسمه تعالی

عنوان مستند

محافظت سیستم در برابر باج‌افزارها

فهرست مطالب

۱ مقدمه

باج‌افزار یک نوع نرم‌افزار مخرب (بدافزار) است که تمام داده‌ها را روی رایانه یا دستگاه تلفن همراه رمزگذاری کرده و دسترسی مالک آن‌ها را به این داده‌ها مسدود می‌کند. هنگامی‌که این آلودگی اتفاق می‌افتد، قربانی پیامی دریافت می‌کند که در آن دستورالعمل‌های چگونگی پرداخت باج (معمولاً در بیت کوین‌ها) ارائه شده است. فرآیند اخاذی اغلب شامل محدودیت زمانی برای پرداخت می‌شود. پرداخت جریمه باید کلید رمزگشایی را به قربانی بدهد، اما هیچ تضمینی وجود ندارد که این اتفاق بیفتد.

۱-۱ دو نوع باج‌افزار رایج وجود دارد

۱. باج‌افزار رمزگذاری، که شامل الگوریتم‌های رمزنگاری پیشرفته است. این برنامه برای مسدود کردن فایل‌های سیستم و تقاضای باج است و برای دسترسی قربانی به آن‌ها، کلیدی وجود دارد که می‌تواند محتوای مسدود شده را رمزگشایی کند. مثلاً CryptoLocker، Locky، CrytpoWall.

۲. باج‌افزار مسدودکننده، که قربانی را به‌وسیله سیستم‌عامل مسدود می‌کند و امکان دسترسی به دسک‌تاپ و هر برنامه یا فایلی را غیرممکن می‌سازد. پرونده‌ها در این مورد رمزگذاری نمی‌شوند، اما مهاجمان باز هم برای کامپیوتر آلوده باج‌گیری می‌کنند. مثلاً باج‌افزار police-theme یا Winlocker.

برخی از نسخه‌های مسدودکننده می‌توانند حتی Master Boot Record(MBR) را آلوده کنند. MBR بخشی از هارددیسک کامپیوتر است که باعث می‌شود سیستم‌عامل بوت شود. هنگامی‌که باج‌افزار MBR رخ بدهد، فرآیند بوت نمی‌تواند به‌طورمعمول انجام شود و باعث می‌شود اعلانی بر روی صفحه، نمایش داده شود. مثلاً خانواده‌های Satana و Petya.

باج‌افزار دارای برخی ویژگی‌های کلیدی است که آن را از دیگر نرم‌افزارهای مخرب مجزا می‌کند.

- از ویژگی‌های آن رمزگذاری غیرقابل شکستن است، این بدان معنی است که شما نمی‌توانید فایل‌ها را خودتان رمزگشایی کنید (ابزارهای رمزگشایی مختلف وجود دارد که توسط محققان امنیت سایبری منتشر شده‌اند).
- باج‌افزار می‌تواند انواع فایل‌ها، از اسناد تا تصاویر، فیلم‌ها، فایل‌های صوتی و سایر مواردی که ممکن است بر روی رایانه باشد، رمزگذاری کند.

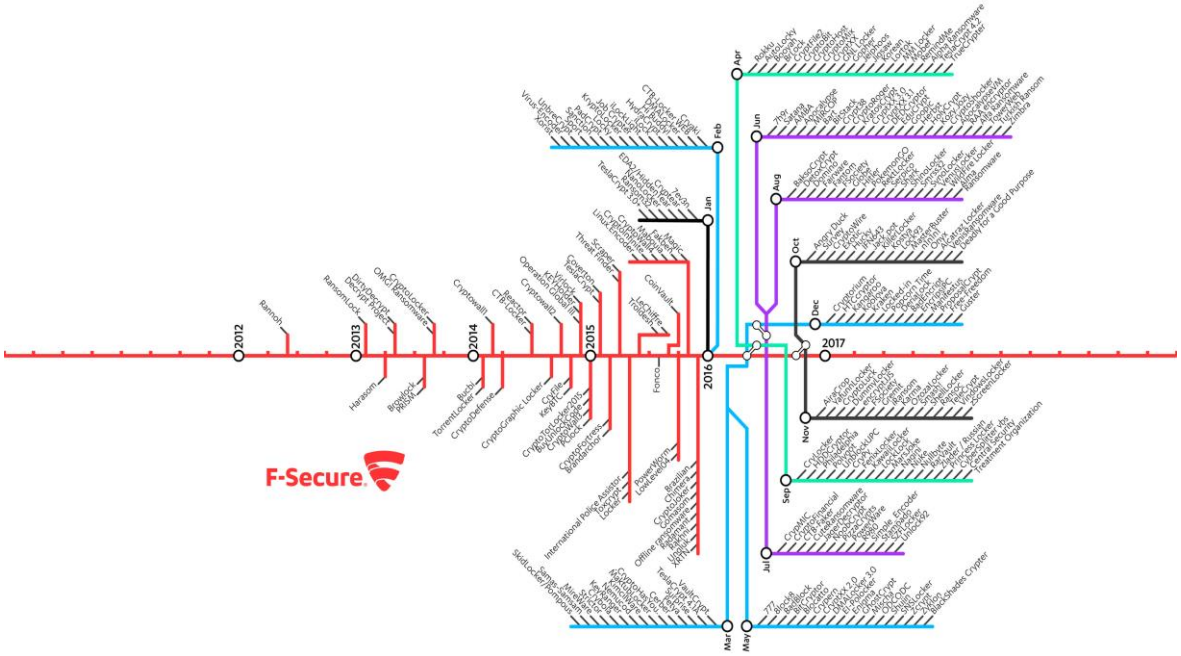
- باج‌افزار می‌تواند نام فایل‌ها را رمزگذاری کند، بنابراین نمی‌توان فهمید کدام اطلاعات تحت تأثیر قرارگرفته‌اند. این یکی از ترفندهای مهندسی اجتماعی است که برای جلب‌توجه و قربانی کردن قربانیان برای پرداخت باج استفاده می‌شود.
- باج‌افزار یک افزونه متفاوت به فایل‌ها اضافه خواهد کرد، و گاهی اوقات یک نوع خاصی از آسیب، باج‌افزار را سیگنال می‌کند.
- باج‌افزار تصویر یا پیامی را نشان می‌دهد که نشان‌دهنده رمزگذاری‌شدن اطلاعات شما هست و برای بازگرداندن آن‌ها مبلغ خاصی را از شما درخواست می‌کند.
- باج‌افزار درخواست پرداخت در Bitcoins را می‌دهد، زیرا این رمزنگاری نمی‌تواند توسط محققان امنیتی سایبری یا سازمان‌های قانونی انجام شود.
- معمولاً این باج‌گیری‌ها محدودیت زمانی دارند تا سطح دیگری از محدودیت‌ها برای این طرح اخاذی، اضافه شود. معمولاً گذشت از زمان سررسید به معنای افزایش باج است، اما این می‌تواند بدین معنا باشد که اطلاعات ناقص شده یا برای همیشه از بین رفته است.
- باج‌افزار از مجموعه پیچیده‌ای از تکنیک‌های گریز از آنتی‌ویروس‌های سنتی استفاده می‌کند.
- باج‌افزار اغلب رایانه‌های آلوده به بات‌نت را جذب می‌کند، بنابراین مجرمان اینترنتی می‌توانند زیرساخت‌های خود را افزایش دهند و حملات آینده را تقویت کنند؛
- باج‌افزار می‌تواند به دیگر رایانه‌های شخصی متصل به شبکه محلی انتشار یابد و باعث ایجاد آسیب بیشتر شود.
- باج‌افزار اغلب قابلیت‌های exfiltration داده‌ها را نشان می‌دهد که بدین معنا است که می‌تواند داده‌ها (نام‌های کاربری، رمزهای عبور، آدرس‌های ایمیل، و غیره) را از کامپیوتر آسیب‌دیده استخراج کند و آن‌ها را به یک سرور تحت کنترل مجرمان سایبری ارسال کند. رمزگذاری فایل‌ها همیشه مرحله نهایی نیست.

۱-۲ یک تاریخچه سریع از باج‌افزار

شاید تصور آن دشوار باشد، اما اولین باج‌افزار در سال ۱۹۸۹ ظاهر شد. این تروجان ایدز نامیده می‌شد، که امروزه عملیات modus آن را خنثی می‌کند. باج‌افزار از طریق فلاپی دیسک پخش شد.

ظهور بیت‌کوین و تکامل الگوریتم‌های رمزنگاری، باعث شد که باج‌افزار از یک تهدید جزئی که در خرابکاری‌های سایبری استفاده می‌شد، به یک ماشین پول‌سازی کامل، تبدیل شود.

نمودار زیر نشان می‌دهد که محققان چند نوع رمزگذاری مخرب در ۱۰ سال گذشته کشف کرده‌اند.



۳-۱ چرا سازندگان و توزیع‌کنندگان باج‌افزار، کاربران خانگی را هدف قرار می‌دهند:

۱. چون آن‌ها پشتیبان‌گیری داده‌ها را ندارند.

۲. چون آن‌ها آموزش امنیت سایبری ندیده‌اند، و ممکن است بر روی هر چیزی کلیک کنند.

۳. چون کمبود دانش امنیتی آنلاین، باعث می‌شود تا مهاجمان سایبری بتوانند به‌راحتی دسترسی به اطلاعات‌شان داشته باشند.

۴. چون آن‌ها حتی امنیت پایه سایبری را ندارند.

۵. چون آن‌ها نرم‌افزار خود را به‌روز نگه نمی‌دارند.

۶. چون آن‌ها موفق به سرمایه‌گذاری در راه‌حل‌های امنیت سایبری نشده‌اند.

۷. چون آن‌ها به شانس اعتقاد دارند تا آن‌ها را امن نگه دارد.

۸. چون اکثر کاربران خانگی هنوز به‌طور انحصاری به آنتی‌ویروس اعتماد می‌کنند تا از همه تهدیدات محافظت شوند که اغلب در تشخیص و توقف باج‌افزار ناکارآمد هستند.

۹. چون بخش زیادی از کاربران اینترنتی، می‌توانند قربانیان بالقوه شوند.

۴-۱ چرا سازندگان و توزیع‌کنندگان باج‌افزار، کسب‌وکارها را هدف قرار می‌دهند:

۱. چون در کسب‌وکارها پول زیادی وجود دارد.

۲. چون مهاجمان می‌دانند که یک آلودگی موفق می‌تواند باعث اختلال در کسب‌وکار بزرگ شود، و شانس آن‌ها جهت دریافت پول افزایش می‌یابد.

۳. چون سیستم‌های کامپیوتری در شرکت‌ها اغلب پیچیده و مستعد آسیب‌پذیری هستند که می‌توانند از طریق وسایل فنی مورد سوءاستفاده قرار گیرند.

۴. چون عامل انسانی هنوز یک مسئولیت بزرگ است که می‌تواند مورد سوءاستفاده قرار گیرد، اما از طریق تاکتیک‌های مهندسی اجتماعی.

۵. چون باج‌افزار با نفوذ به هسته کسب‌وکار، می‌تواند نه‌تنها کامپیوترها را بلکه سرورها و سیستم‌های به اشتراک‌گذاری فایل مبتنی بر ابر را نیز تحت تأثیر قرار دهد.

۶. چون کسب‌وکارهای کوچک اغلب آماده برای مقابله با حملات پیشرفته سایبری نیستند.

۵-۱ چرا سازندگان و توزیع‌کنندگان باج‌افزار، نهادهای دولتی را هدف قرار می‌دهند:

۱. چون مؤسسات دولتی مانند ادارات دولتی، پایگاه‌های اطلاعاتی عظیم شخصی و محرمانه را مدیریت می‌کنند که مجرمان سایبری می‌توانند آن‌ها را به فروش برسانند.

۲. چون کاهش بودجه و مدیریت غیرمستقیم اغلب بر بخش‌های سایبری تأثیر می‌گذارد.

۳. چون کارکنان برای کشف و جلوگیری از حملات سایبری آموزش ندیده‌اند (نرم‌افزارهای مخرب اغلب از تاکتیک‌های مهندسی اجتماعی برای سوءاستفاده از ناهنجاری‌های انسانی و ضعف‌های روحی استفاده می‌کنند).

۴. چون مؤسسات دولتی اغلب از نرم‌افزار و تجهیزات قدیمی استفاده می‌کنند، بدان معنی که سیستم‌های کامپیوتری آن‌ها با حفره‌های امنیتی، پیکربندی می‌شود و مورد سوءاستفاده قرار می‌گیرند.

۵. چون یک آلودگی موفق تأثیر زیادی بر انجام فعالیت‌های معمول دارد و باعث اختلالات زیادی می‌شود.

۶. چون حمله موفقیت‌آمیز به نهادهای دولتی، جنایتکاران سایبری را برای حملات بیشتر وسوسه می‌کند.

۲ چگونه تهدیدات باج‌افزار گسترش می‌یابد؟

مجرمان سایبری به‌سادگی، ساده‌ترین راه برای آلوده‌کردن یک سیستم یا شبکه را دنبال می‌کنند و از این بدافزار برای گسترش محتوای مخرب استفاده می‌کنند.

۲-۱ رایج‌ترین روش‌های آلوده‌سازی که توسط مجرمان سایبری مورد استفاده قرار می‌گیرد:

- ایمیل هرزنامه که حاوی لینک‌های مخرب یا فایل‌های ضمیمه هستند.
- سوءاستفاده امنیتی از نرم‌افزار آسیب‌پذیر.
- ترافیک اینترنت به وب‌سایت‌های مخرب هدایت می‌شود.
- وب‌سایت‌های قانونی که کد مخرب به صفحات وب آن‌ها تزریق شده است.
- دانلود درایو.
- کمپین‌های تبلیغاتی.
- پیام‌های اس‌ام‌اس (هنگام استفاده از دستگاه‌ها تلفن همراه).
- بات‌نت‌ها.
- propagation (گسترش از یک کامپیوتر آلوده به دیگری)؛ به‌عنوان‌مثال Wanna Cry، از استخراج کیت استفاده می‌کند تا یک کامپیوتر را اسکن کند، و سپس با استفاده از یک آسیب‌پذیری خاص یک حمله باج‌افزار را ترتیب می‌دهد.
- برنامه‌های وابسته به سرویس باج‌افزار. اساساً، توسعه‌دهنده پشت باج‌افزار هر بار که از کاربر باج می‌گیرد، از هرگونه سودی بهره می‌گیرد.

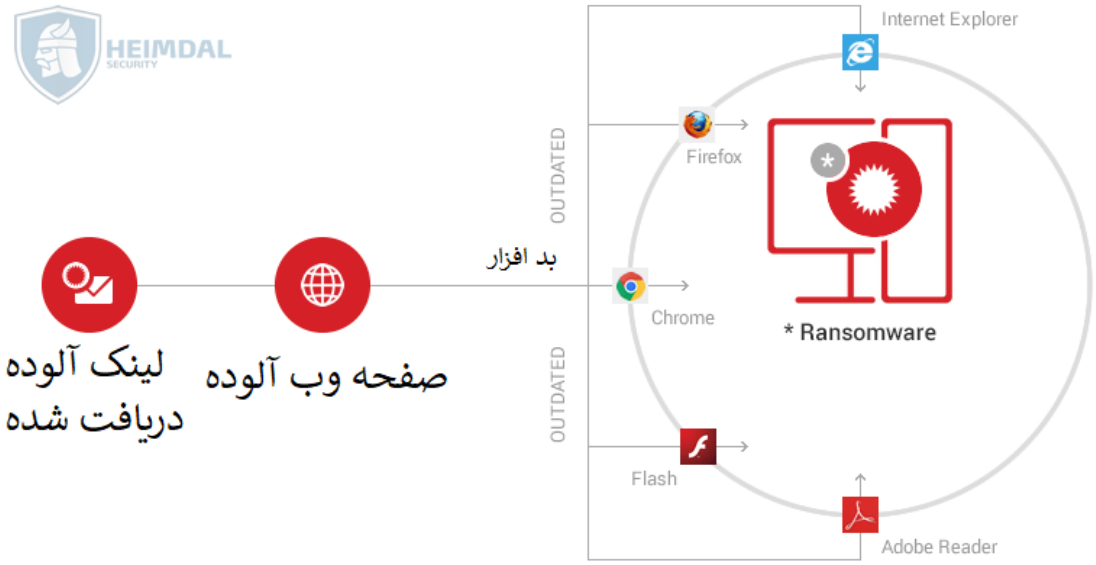
۲-۲ حملات باج‌افزار Crypto ترکیب ظریفی از تکنولوژی و دست‌کاری روانی است(همچنین به‌عنوان مهندسی اجتماعی شناخته می‌شود).

این حملات روزبه‌روز گسترش می‌یابند، زیرا مجرمان سایبری از اشتباهات‌شان یاد می‌گیرند و کد مخرب خود را به کار می‌برند تا در برابر راه‌حل‌های امنیتی سایبری، قوی‌تر کنند. حمله WannaCry یک مثال

کامل از این نمونه است؛ زیرا از یک آسیب‌پذیری گسترده ویندوز استفاده می‌کند تا کامپیوتر را بدون هیچ‌گونه تعامل با کاربر آلوده کند.

۳ چگونه آلودگی به باج‌افزار اتفاق می‌افتد؟

اگرچه مراحل آلودگی به هر نسخه باج‌افزار کمی متفاوت است، اما موارد اصلی آن شامل مراحل زیر است.



۱. در ابتدا، قربانی یک ایمیل دریافت می‌کند که شامل یک لینک مخرب یا یک پیوست بدافزار است. به همین ترتیب، این آلودگی می‌تواند از یک وب‌سایت مخرب ناشی از یک سوءاستفاده امنیتی برای ایجاد Backdoor بر روی کامپیوتر قربانی با استفاده از یک نرم‌افزار آسیب‌پذیر ایجاد شود.

۲. اگر قربانی روی پیوند کلیک کند یا فایل پیوست را دریافت کند و آن را باز کند، downloader روی کامپیوتر آسیب‌دیده قرار می‌گیرد.

۳. downloader از لیست دامنه‌ها یا سرورهای C&C تحت کنترل مجرمان سایبری استفاده می‌کند تا برنامه باج‌افزار را دانلود کند.

۴. سرور فراخوانی شده C&C با ارسال فایل (داده‌های) درخواست‌شده، پاسخ می‌دهد.

۵. بدافزار پس از آن کل محتوای هارددیسک، فایل‌های شخصی و اطلاعات حساس را رمزگذاری می‌کند. همه‌چیز، ازجمله داده‌های ذخیره‌شده در حساب‌های ابری (Google Drive، Dropbox) روی کامپیوتر همگام‌سازی شده‌اند. همچنین بدافزار می‌تواند داده‌ها را در رایانه‌های دیگر متصل به شبکه محلی رمزگذاری کند.

۶. هشداری با دستورالعمل چگونگی پرداخت برای کلید رمزگشایی، بر روی صفحه‌نمایش ظاهر می‌شود.

۴ طرح حفاظت ضد باج‌افزار

راهنمایی‌های حفاظتی به چهار دسته، سازمان‌دهی شده‌اند، بنابراین با عمل به آن‌ها می‌توان از حملات باج‌افزاری جلوگیری کرد:

- مواردی که باید در کامپیوتر انجام شود.
- مواردی که باید در مرورگر انجام شود.
- مواردی که باید به‌صورت آنلاین انجام شود.
- ابزارهای امنیتی ضد باج‌افزار.

۱-۴ مواردی که باید در کامپیوتر انجام شود:

۱. اطلاعات مهم فقط بر روی کامپیوتر ذخیره نشوند.

داده‌های غیرقابل تعویض مانند مدارک تحصیلی، اسناد کاری و عکس‌های گران‌قیمت فقط کامپیوتر شما را آسیب‌پذیر می‌سازد. اگر اتفاقی در این دستگاه رخ بدهد، همه‌چیز از بین خواهد رفت.

۲. دو backup از داده‌ها باید ذخیره شود.

یک کپی از اطلاعات خود را در یک هارددیسک خارجی و یک کپی در ابر نگه‌دارید مثلاً Dropbox، Google Drive و غیره. اطمینان حاصل کنید که اطلاعات شما به‌روز باشند. و بررسی کنید که پشتیبان‌گیری شما درست باشد و می‌توانید آن را دوباره بازگردانید.

۳. برنامه‌های Dropbox، Google Drive و OneDrive نباید به‌طور پیش‌فرض باز باشند.

فقط یک‌بار در روز باید آن‌ها را بازکرد تا داده‌ها همگام‌سازی شوند و پس از انجام این کار مجدداً بسته شوند. انواع باج‌افزار وجود دارد که می‌تواند همه‌چیز را بر روی درایو شما رمزگذاری کند، ازجمله داده‌ها در حساب‌های ابری. باج‌افزار می‌تواند پشتیبان‌گیری داده‌ها را نابود کند، به همین دلیل باید مراقب باشید و چندین پشتیبان را نگه‌دارید.

۴. سیستم‌عامل و نرم‌افزارها باید به‌روز نگه‌داشته شوند و شامل آخرین به‌روزرسانی‌های امنیتی باشند.

آخرین به‌روزرسانی‌های امنیتی بسیار مهم هستند. اگر آخرین به‌روزرسانی‌ها را اعمال کنید، می‌توانید از پچ‌های امنیتی استفاده کنید که آسیب‌پذیری زیادی را حل می‌کنند. به همین دلیل است که متخصصان امنیت سایبری به پچ کردن اصرار دارند.

۵. برای استفاده‌ی روزانه نباید از حساب کاربری admin استفاده شود. باید از حساب کاربری میهمان با دسترسی محدود استفاده شود.

زمانی که از یک حساب مهمان استفاده شود، اگر با باج‌افزار و یا نوع دیگری از نرم‌افزارهای مخرب مواجه شدید، می‌توانید خسارات را محدود کنید.

۶. باید ماکروها و ActiveX در مجموعه میکروسافت آفیس(Word، Excel، PowerPoint و غیره) مسدود باشند.

این‌ها قطعات نرم‌افزاری هستند که مجرمان سایبری اغلب برای گسترش نرم‌افزارهای مخرب و آلودگی به رایانه‌ها استفاده می‌کنند. اسناد آلوده به‌شدت در حملات سایبری مورداستفاده قرار می‌گیرند، زیرا آن‌ها قادر به مخفی‌کردن افکار مخرب مجرمان هستند. اگر آن‌ها مفید یا بی‌خطر باشند، قربانیان بیشتر مایل به باز کردن آن‌ها هستند.

۷. قبل از کلیک برروی افزونه‌های فایل، آن‌ها را تائید کنید.

مجرم سایبری فایل‌ها را دست‌کاری می‌کند تا آن‌ها بی‌ضرر باشند. هدف این است که شما را وادار به کلیک روی آن‌ها کند و یک آلودگی مخرب را که بر کامپیوتر شما غلبه می‌کند، راه‌اندازی کند. تنظیمات ویندوز خود برای نشان دادن پسوندهای نام فایل، تنظیم کنید، بنابراین شما متوجه فرمت‌های مشکوک، مانند .jpeg.exe می‌شوید که باید از باز کردن آن‌ها اجتناب کنید.(که آن‌ها یک تصویر نیستند، و فایل‌های اجرایی مخرب هستند).

۸. ویژگی AutoPlay را بر روی کامپیوتر خود غیرفعال کنید.

AutoPlay یک ویژگی ویندوز است که به شما اجازه می‌دهد فوراً رسانه‌های دیجیتال (کارت‌های USB، CDها، دوربین‌های دیجیتال) را با یک برنامه مشخص‌شده، بازکنید. بدافزار می‌تواند از این گزینه برای دسترسی به رایانه شما استفاده کند و به‌طور خودکار شروع به کار کند، بنابراین بهتر است این گزینه را غیرفعال نگه‌دارید.

۹. بی‌سیم و بلوتوث را روشن نکنید مگر اینکه شما بخواهید از آن استفاده کنید.

اتصالات ناامن می‌تواند به شما بهای زیادی بپردازد، بنابراین اگر از آن‌ها استفاده نمی‌کنید، اتصال بی‌سیم و بلوتوث خود را خاموش‌کنید. مجرمان سایبری می‌توانند از هر دو این اتصالات برای حمله و تصاحب دستگاه‌های شما استفاده کنند. این قانون برای تمام دستگاه‌های شما سازگار است نه‌فقط برای کامپیوتر شما.

۱۰. چندین کامپیوتر را در یک شبکه محلی قرار ندهید.

باج‌افزار، بسیار پیشرفته و قادر به گسترش به دیگر کامپیوترهای متصل در یک شبکه محلی است. اگر یک کامپیوتر آلوده شود، اما به دیگر کامپیوترها متصل نباشد، آلودگی گسترش نخواهد یافت.

۱۱. هرگز USBای که منبع آن معلوم نیست را به یک دستگاه وصل نکنید.

USB را متصل نکنید حتی اگر آن را با آنتی‌ویروس اسکن می‌کنید، زیرا آنتی‌ویروس گاهی اوقات خطرناک‌ترین حملات باج‌افزار را به‌درستی تشخیص نمی‌دهد. فقط می‌توانید از USBهایی که منبع آن مشخص هست و محتویات آن را می‌شناسید، استفاده کنید.

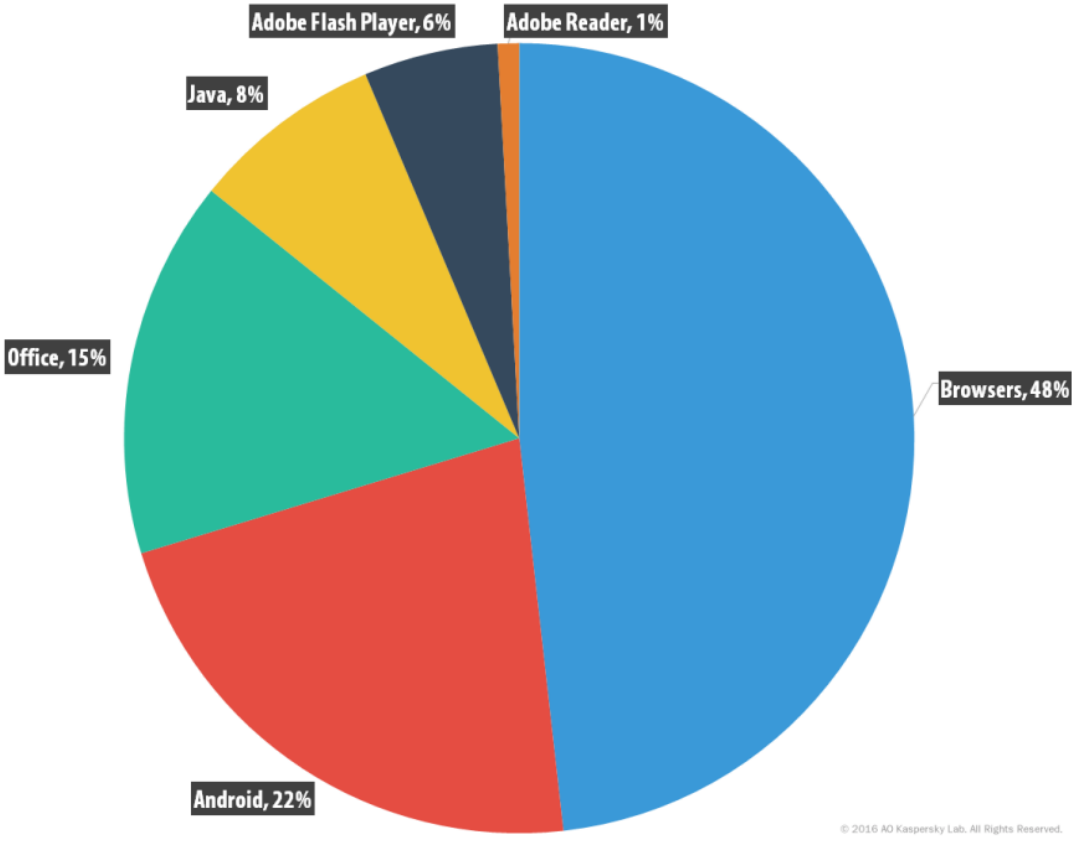
۱۲. اگر از ویندوز PowerShell استفاده نمی‌کنید، آن را غیرفعال کنید.

اگر از PowerShell برای وظایف خود استفاده نمی‌کنید، آن را غیرفعال کنید. انواع مختلفی از نرم‌افزارهای مخرب ازجمله باج‌افزار وجود دارند، که از PowerShell سوءاستفاده می‌کنند و از آن برای ساخت و اجرای بدافزار در دستگاه‌های قربانی استفاده می‌کنند.

۲-۴ مواردی که باید بر روی مرورگر انجام شوند:

۱. پلاگین‌های زیر باید از مرورگرها حذف شوند:

Adobe Flash، Adobe Reader، Java و Silverlight باید از مرورگرها حذف شوند. باید مرورگر را تنظیم کنید تا هرزمانی که نیاز به استفاده از این پلاگین‌ها هست، از شما بپرسد که آیا آن پلاگین را فعال کند یا خیر؟ این چهار پلاگین برای حملات سایبری مورد سوءاستفاده قرار می‌گیرند، چنانچه در آمار زیر می‌توانید ببینید.



۲. تنظیمات امنیتی و حریم خصوصی مرورگرها باید برای افزایش امنیت تنظیم شوند.

کارهای زیادی وجود دارند که با انجام آن‌ها مرورگرهای‌تان ایمن‌تر می‌شوند. این نوع تنظیمات چندین دقیقه طول می‌کشند و تفاوت زیادی را ایجاد می‌کنند.

۳. پلاگین‌ها و افزونه‌های قدیمی باید از مرورگرهای‌تان حذف شوند.

تنها افزونه‌هایی که لازم هست باید نگه‌داشته شوند و باید به آخرین نسخه نیز به‌روزرسانی شوند. پلاگین‌ها و افزونه‌های قدیمی می‌توانند بدون اجازه شما شروع به فعالیت کنند.

۴. از یک مسدودکننده تبلیغاتی برای جلوگیری از تهدید تبلیغات بالقوه مخرب، استفاده شود.

Malvertising یک تهدید بسیار جدی است. مهاجمان اغلب از کمپین‌های تبلیغاتی برای آسیب به قربانیان استفاده می‌کنند. راه محافظت از خود در برابر این خطر، استفاده از یک مسدودکننده تبلیغاتی است.

۳-۴ مواردی که آنلاین باید انجام شوند:

۱. هرگز نباید ایمیل‌های اسپم یا ایمیل‌های با فرستنده ناشناس بازشوند.

اگر نمی‌دانید چه کسی ایمیل را فرستاده، آن را حذف کنید یا آن را مستقیماً به هرزنامه بفرستید. اگر مطمئن نیستید که آیا باید آن را بازکنید، مستقیماً با فرستنده تماس بگیرید و اطلاعات را تأیید کنید. ایمیل‌های هرزنامه بیشترین تاکتیک استفاده‌شده برای گسترش باج‌افزار است.

۲. هرگز نباید پیوندها را از ایمیل‌های اسپم یا ایمیل‌های مشکوک دانلود کرد.

این رایج‌ترین نوع آلوده‌کردن رایانه‌ها با رمزگذاری نرم‌افزارهای مخرب است. قربانی یک فایل ضمیمه مخرب را بارگیری و باز می‌کند و پس از آن جنجال به راه می‌افتد.

۳. هرگز نباید روی ایمیل‌های اسپم یا ایمیل‌های مشکوک کلیک کرد.

لینک‌های این ایمیل‌ها در حملات باج‌افزار استفاده می‌شوند. فقط روی آن‌ها کلیک نکنید و اگر از آن لینک مطمئن نیستید، ابزارهای زیادی وجود دارد که می‌توانید برای تصدیق امن‌بودن آن لینک استفاده کنید. اما فقط به این تصدیق بسنده نکنید.

همچنین، از کلیک‌کردن روی لینک‌های عجیب‌وغریب در رسانه‌های اجتماعی، لینک‌های دریافت شده از طریق اسکایپ و دیگر سرویس‌های پیام‌رسانی فوری (WhatsApp، Viber و غیره) جلوگیری کنید. آن‌ها می‌توانند به داده‌ها و دستگاه شما آسیب برسانند.

۴. یادگیری تشخیص ایمیل‌هایی که وانمود می‌کنند که از شرکت‌های مطمئن هستند.

مهاجمان سایبری اغلب هویت شرکت‌های بزرگ را جعل می‌کنند تا افراد با باز کردن ایمیل‌های مخرب و یا کلیک بر روی لینک‌های آلوده و دانلود فایل‌های مخرب آلوده شوند. ازآنجاکه افراد به علامت‌های تجاری مانند شرکت‌های مخابراتی، ارائه‌دهندگان خدمات اینترنتی، پست‌های محلی و غیره اعتماد دارند، تمایل دارند روی لینک‌های آنها کلیک کنند و فایل‌های پیوست را باز کنند بدون این‌که فکر کنند که آن‌ها خطرناک و مخرب هستند.

۴-۴ ابزارهای امنیتی ضد باج‌افزار:

۱. از آنتی‌ویروس قابل‌اعتماد استفاده شود که ماژول‌های به‌روزرسانی خودکار و اسکنر بلادرنگ دارد.

این آنتی‌ویروس را به‌روز نگهدارید و توجه داشته باشید که یک آنتی‌ویروس رایگان هرگز حفاظت در آن سطحی که یک آنتی‌ویروس پولی، فراهم می‌کند را ارائه نمی‌دهد. این بخش مهمی از طرح حافظت از اطلاعات است.

۲. ویندوز Firewall را فعال کنید و آن را روشن نگه‌دارید.

داشتن Firewall یک تدبیر امنیتی مناسب است، البته شما می‌توانید از دیگر راه‌حل‌های Firewall به‌خوبی استفاده کنید.

۳. راه‌حل فیلتر ترافیک، می‌تواند امنیت ضد باج‌افزار را فعال کند.

۵ چگونه حملات باج‌افزار را تشخیص دهیم:

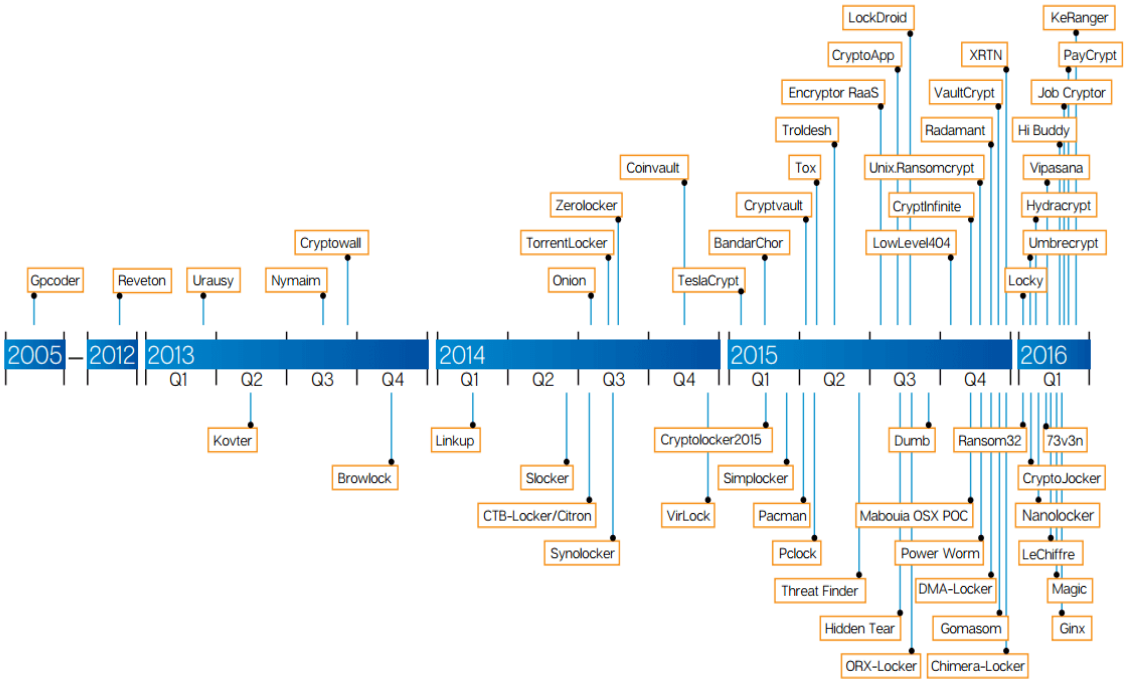
برخی از انواع باج‌افزار در هنگام رمزگذاری اطلاعات سریع عمل می‌کنند، اما بعضی دیگر، کند عمل می‌کنند. اگر متوجه شدید که نمی‌توان به برخی از فایل‌ها دسترسی پیدا کرد، و در حال حاضر فایل‌ها یک فرمت عجیب‌وغریب دارند، لازم است موارد زیر را انجام دهید

- بلافاصله اینترنت قطع شود! بی‌سیم خاموش شود و یا کابل اترنت از کامپیوتر جدا شود.
- باید بررسی شود که تا چه حد آلودگی گسترش یافته است و چندین فایل رمزگذاری شده است.

- بررسی کنید که آیا پشتیبان اطلاعات شما بر روی یک کامپیوتر دیگر که امن است، کار می‌کند یا خیر؟
- ازآنجا که باج‌افزار ممکن است آلودگی‌های دیگر مانند keyloggers و یا نرم‌افزارهای مخرب مالی را به دنبال داشته باشد یا حتی ممکن است کامپیوتر شما را به دام یک باتنت بیندازد، بهتر است یک سیستم‌عامل سالم مجدداً نصب شود.
- پس از بازیابی سیستم از طریق نسخه پشتیبان یا از طریق نصب مجدد سیستم‌عامل، مراحل بالا را برای جلوگیری از دیگر آلودگی‌های باج‌افزار انجام دهید.

۵-۱ چگونه می‌توان اطلاعات خود را بدون پرداخت جریمه به دست آورد:

صدها نوع باج‌افزار وجود دارد، اما محققان امنیت سایبری بی‌وقفه کار می‌کنند تا حداقل بعضی از رمزگذاری‌هایی که استفاده می‌شوند را بشکنند. متأسفانه خانواده‌های زیادی از باج‌افزارهای معروف وجود دارند که ثابت‌شده‌اند قابل شکستن نیستند. به‌رغم این، بسیاری از انواع cryptoware وجود دارند که به‌خوبی کدگذاری نشده‌اند و قابل کرک هستند.



۵-۲ نحوه شناسایی باج‌افزار که شما را آلوده کرده است:

گاهی اوقات، اعلان باج‌گیری به شما می‌گوید که چه نوع باج‌افزاری، فایل‌های شما را رمزگذاری کرده است، اما این اتفاق می‌تواند بدون دادن هیچ‌گونه اطلاعاتی به شما رخ دهد. بسیاری از افزونه‌ها، نشان

داده‌اند که انواع جدیدی از نرم‌افزارهای مخرب رمزگذاری وجود دارند که رمزگشایی‌ای برای آن‌ها در دسترس نیست.

اگر شما نیاز به کمک برای شناسایی اینکه چه نوع باج‌افزاری سیستم شما را آلوده کرده است، دارید دو ابزار بعدی وجود دارد که می‌توانید استفاده کنید:

Crypto Sheriff from No More Ransom

ID Ransomware from MalwareHunter Team

لطفاً قبل از استفاده از آن‌ها شرایط ویژه استفاده از این ابزارها را نیز مطالعه کنید.

۵-۳ ابزارهای رمزگشایی باج‌افزار

این ابزارهای رایگان به شما کمک می‌کند تا اطلاعات خود را بدون پرداخت جریمه رمزگشایی کنید.

جهت رفع تکلیف، لیست زیر فقط یک نقطه‌ی شروع است. از آن استفاده می‌شود، اما باید یک تحقیق کم در مورد آن انجام شود. رمزگشایی امن داده‌ها یک فرایند اعصاب‌خردکن است، بنابراین باید تا حد امکان کامل انجام شود.

تمام تلاش‌ها انجام می‌شود تا لیست زیر به‌روز باشد، اما احتمالاً هرگز قطعی نخواهد بود.

استفاده از بعضی از ابزارهای رمزگشایی ذکرشده‌ی زیر آسان است، درحالی‌که بعضی دیگر از آن‌ها نیاز به دانش فنی کمی برای شکستن دارند. شما می‌توانید از یکی از این فروم‌های حذف بدافزار که دارای اطلاعات زیاد و جامعی هستند، کمک بگیرید.

۵-۳-۱ لیست ابزارهای رمزگشایی باج‌افزار

OpenToYou decryption tools
Globe۳ decryption tool
Dharma Decryptor
CryptON decryption tool
Alcatraz Decryptor tool // direct tool download
HiddenTear decryptor (Avast)
NoobCrypt decryptor (Avast)
CryptoMix/CryptoShield decryptor tool for offline key (Avast)
Damage Ransomware decryption tool
.۷۷۷ Ransomware decrypting tool
۷even-HONE$T decrypting tool

.۸lock۸ Ransomware decrypting tool + explanations

۷ev۳n decrypting tool

Agent.iih decrypting tool (رمزگشایی‌شده است Rakhni Decryptor توسط)

Alma decrypting tool
Al-Namrood decrypting tool
Alpha decrypting tool
AlphaLocker decrypting tool
Apocalypse decrypting tool
ApocalypseVM decrypting tool + alternative
Aura decrypting tool (رمزگشایی‌شده است Rakhni Decryptor توسط)

AutoIt decrypting tool (رمزگشایی‌شده است Rakhni Decryptor توسط)

Autolocky decrypting tool
Badblock decrypting tool + alternative ۱

Bart decrypting tool
BitCryptor decrypting tool
BitStak decrypting tool
Chimera decrypting tool + alternative ۱ + alternative ۲

CoinVault decrypting tool
Cryaki decrypting tool (رمزگشایی‌شده است Rakhni Decryptor توسط)

Crybola decrypting tool (رمزگشایی‌شده است Rakhni Decryptor توسط)

CrypBoss decrypting tool
Crypren decrypting tool
Crypt۳۸ decrypting tool

Crypt۸۸۸ (see also Mircop) decrypting tool

CryptInfinite decrypting tool
CryptoDefense decrypting tool
CryptoHost (a.k.a. Manamecrypt) decrypting tool
Cryptokluchen decrypting tool (رمزگشایی‌شده است Rakhni Decryptor توسط)

CryptoTorLocker decrypting tool
CryptXXX decrypting tool
CrySIS decrypting tool (رمزگشایی‌شده است Rakhni Decryptor توسط)

CTB-Locker Web decrypting tool
Cute Ransomware decrypting tool
DeCrypt Protect decrypting tool

Democry decrypting tool (رمزگشایی‌شده است Rakhni Decryptor توسط)
DMA Locker decrypting tool + DMA۲ Locker decoding tool
Fabiansomware decrypting tool
Encryptile decrypting tool
FenixLocker – decrypting tool
Fury decrypting tool (رمزگشایی‌شده است Rakhni Decryptor توسط)
GhostCrypt decrypting tool
Globe / Purge decrypting tool + alternative
Gomasom decrypting tool
Harasom decrypting tool
HydraCrypt decrypting tool
Jaff decrypter tool
Jigsaw/CryptoHit decrypting tool + alternative
KeRanger decrypting tool
KeyBTC decrypting tool
KimcilWare decrypting tool
Lamer decrypting tool (رمزگشایی‌شده است Rakhni Decryptor توسط)
LeChiffre decrypting tool + alternative
Legion decrypting tool
Linux.Encoder decrypting tool
Lock Screen Ransomware decrypting tool
Locker decrypting tool
Lortok decrypting tool (رمزگشایی‌شده است Rakhni Decryptor توسط)
MarsJoke decryption tool
Manamecrypt decrypting tool (a.k.a. CryptoHost)
Mircop decrypting tool + alternative
Merry Christmas / MRCR decryptor
Nanolocker decrypting tool
Nemucod decrypting tool + alternative
NMoreira Ransomware decryption tool
ODCODC decrypting tool
Operation Global III Ransomware decrypting tool
Ozozalocker ranomware decryptor
PClock decrypting tool
Petya decrypting tool + alternative
Philadelphia decrypting tool
PizzaCrypts decrypting tool

Pletor decrypting tool (توسط Rakhni Decryptor رمزگشایی‌شده است)
Pompous decrypting tool
PowerWare / PoshCoder decrypting tool
Radamant decrypting tool
Rakhni decrypting tool
Rannoh decrypting tool
Rector decrypting tool
Rotor decrypting tool (توسط Rakhni Decryptor رمزگشایی‌شده است)
Scraper decrypting tool
Shade / Troldesh decrypting tool + alternative
SNSLocker decrypting tool
Stampado decrypting tool + alternative
SZFlocker decrypting tool
TeleCrypt decrypting tool (additional details)
TeslaCrypt decrypting tool + alternative ۱ + alternative ۲
TorrentLocker decrypting tool
Umbrecrypt decrypting tool
Wildfire decrypting tool + alternative
WannaCry decryption tool + Guide
XORBAT decrypting tool
XORIST decrypting tool + alternative

همان‌طور که مشخص است برخی از این ابزارهای رمزگشایی فقط برای چند خانواده از باج‌افزار کار می‌کنند، درحالی‌که آسیب‌هایی دارای بیش از یک راه‌حل هستند (اگرچه این موارد به‌ندرت وجود دارد).

۶ منابع

- https://heimdalsecurity.com/blog/what-is-ransomware-protection/
- https://www.barkly.com/ransomware-protection-and-prevention#section-three
- http://www.itrdntechnologies.com/index.php/blog-categories/blog-network-and-security/۱۶۴-the-rise-of-ransomware-and-۱۰-easy-steps-to-protect-your-system-and-workplace
- https://heimdalsecurity.com/blog/anti-ransomware-protection-plan/
- https://heimdalsecurity.com/blog/ransomware-decryption-tools/