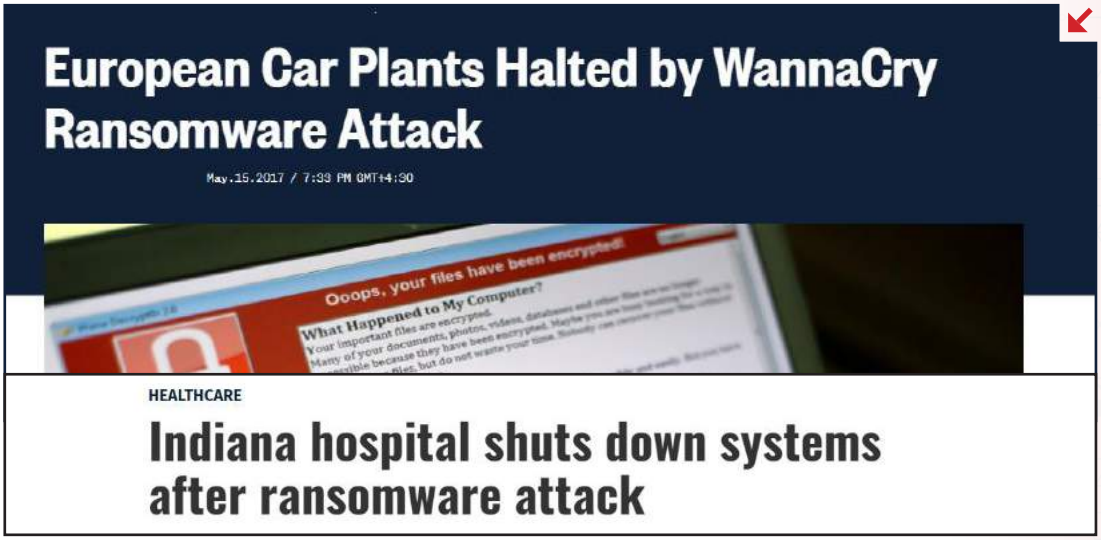
سازمان بورس و اوراق بهادار
Securities & Exchange Organization

بولتن آگاهی رسانی امنیت سایبری، شماره ۵

کابوس از دست دادن فایل‌ها؛ چگونه به دام باج‌افزارها نیفتیم؟

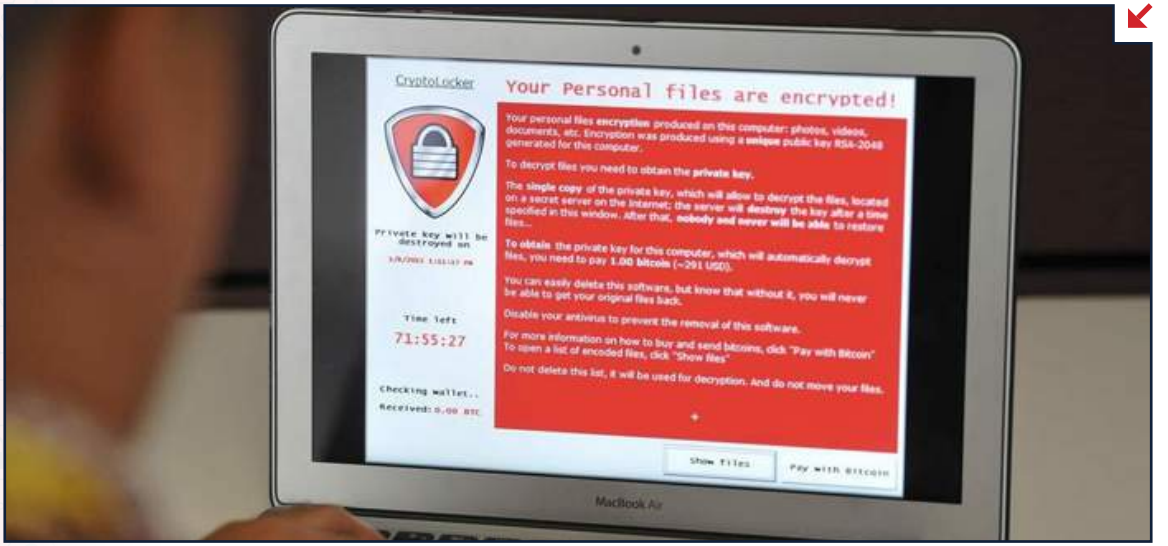
■ مرکز نظارت بر امنیت اطلاعات بازار سرمایه ■

کابوس از دست دادن فایل‌ها: چگونه به دام باج‌افزارها نیفتیم؟



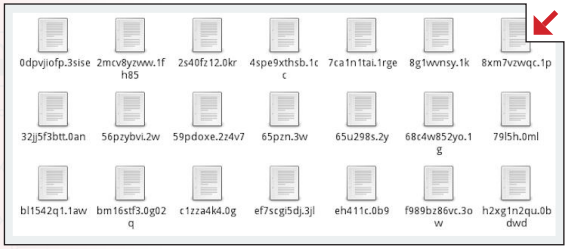
- حمله باج‌افزاری به بیمارستانی در آمریکا و خاموش شدن سیستم‌های بیمارستان
- حمله باج افزاری به کارخانه‌های رنو و نیسان
- حمله باج افزاری به بانک‌های هند

نمونه‌های متعددی از تیترهای خبری فوق وجود دارد و همه نشان از خسارات مادی و اعتباری شرکت‌ها و نهادهای بزرگ در اثر حمله سایبری موسوم به باج افزار (Ransomware) دارد. این نوع حمله در کمین بسیاری از افراد، شرکت‌ها، سازمان‌ها و حتی دولت‌ها است و در صورت عدم اتخاذ راهکارهای پیشگیرانه، می‌تواند خسارات جبران‌ناپذیری ایجاد کند. در این مطلب آموزشی، سعی شده است در خصوص این حمله و راهکارهای پیشگیری از آن توضیحات مفیدی ارائه شود.



باج‌افزار: بدافزار یا ویروسی خطرناک، که اسناد و فایل‌های شما را مورد هدف قرار می‌دهد.

باج‌افزار نوع خاصی از بد افزار است که به طور فعال در حال گسترش در اینترنت است و قربانی (سیستم مورد حمله) را تهدید به از بین بردن مدارک و فایل‌هایش می‌کند. بد افزار یک نرم‌افزار کامپیوتری است که برای انجام کارهای مخرب مورد استفاده قرار می‌گیرد. باج‌افزارها سودآوری زیادی برای تبهکاران دارند. از این رو، استفاده از آن‌ها توسط تبهکاران در حال افزایش است. در صورتی که کامپیوترتان به باج‌افزار آلوده شود، فایل‌های آن توسط هکر، رمزگذاری می‌شود و شما امکان بازکردن و دستیابی به فایل‌های خودتان را نخواهید داشت. پس از این نوع حمله، هکر به شما اطلاع می‌دهد که تنها راهی که می‌توانید مجددا به فایل‌های خود دست یابید، پرداخت پول (باج) به وی است. به همین دلیل به این گونه حملات، باج‌افزار گفته می‌شود. اغلب این باج باید به شکل پول دیجیتال همچون بیت‌کوین (به دلیل غیر قابل ردیابی بودن) پرداخت گردد. به عنوان نمونه، می‌توان به باج‌افزارهای معروف Locky، CryptoLocker و CryptoWall اشاره کرد. در شکل زیر تعدادی فایل بر روی یک کامپیوتر نشان داده شده است که توسط حمله باج‌افزاری آلوده شده‌اند. همانطور که مشاهده می‌کنید، نام فایل‌ها و حتی پسوند آن‌ها نیز تغییر کرده است.

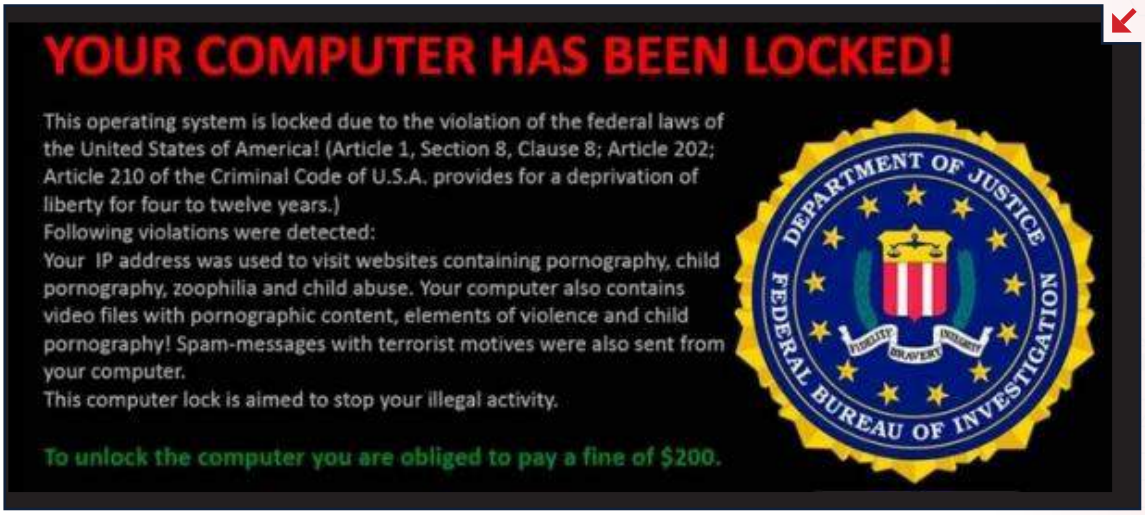


می توان ادعا نمود که اگر باج افزاری فایل‌های شما را رمزنگاری کرد، تقریبا آن‌ها را از دست داده اید؛

به عبارتی، به گزینه پرداخت باج و پس از آن دستیابی به فایل هایتان، خیلی فکر نکنید! مگر اینکه ...

ادامــه را بخوانید

برخی از باج افزارها همچون Satana ،Winlocker و Petya فایل های موجود بر روی کامپیوتر را رمز نمی‌کنند بلکه به گونه‌ای دسترسی به سیستم عامل آن را قفل نموده و کاربر نمی‌تواند وارد سیستم شود. در شکل زیر نمونه‌ای از سیستم آلوده شده به این نوع باج‌افزار را مشاهده نمائید.



رایج ترین روش های انتشار باج افزار

ایمیل مخرب:

رایجترین شیوه انتشار باج‌افزار، فرستادن ایمیل های مخرب به قربانیان است، به گونه‌ای که تبهکار سایبری از شما می‌خواهد فایل پیوست ایمیل ارسالی را باز کنید یا بر روی لینکی که برایتان ارسال کرده است، کلیک نمائید.

فیشینگ:

حملات فیشینگ و تبلیغات اینترنتی نیز منبع دیگری برای انتشار باج افزار هستند، به گونه ای که ترافیک اینترنت کاربر به سمت وب سایت های مخرب هدایت شده و باج افزار به سیستم کاربر نفوذ می کند.

ورود از طریق نرم‌افزار منسوخ:

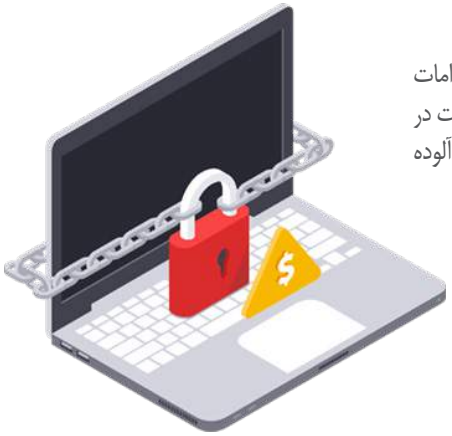
استفاده از نرم‌افزارهای قدیمی و به روزرسانی نشده نیز می‌تواند راهی برای ورود باج‌افزار به سیستم شما باشد. نرم‌افزارهای قدیمی و به‌روزرسانی نشده، اغلب دارای آسیب‌پذیری‌هایی هستند که مهاجمین سایبری شیوه سوءاستفاده از آن‌ها را می‌دانند و از آن برای آلوده کردن سیستم استفاده می کنند.

آیا باید باج را بپردازید؟

سوال سختی است. مشکل این است که هر چه موارد پرداخت باج به این تبهکاران بیشتر شود، با انگیزه بیشتری به حملات خود ادامه خواهند داد. از طرف دیگر، ممکن است راه دیگری برای دسترسی به فایل‌های خود نداشته باشید. در هر حال، آگاه باشید هیچ تضمینی وجود ندارد که با پرداخت باج، بتوانید فایل‌های خود را به دست آورید. مخاطب شما یک تبهکار خواهد بود، ممکن است فایل‌هایتان را رمزگشایی نکنند و حتی ممکن است روش رمزگشائی را در ازای پرداخت پول در اختیار شما قرار دهند اما در طول فرایند رمزگشائی، کامپیوترتان به بدافزارهای دیگری آلوده شود.

مقابله با باج افزارها

مقابله با باج‌افزارها می‌تواند به دو دسته پیشگیرانه و واکنشی تقسیم شود. اقدامات پیشگیرانه به منظور جلوگیری از آلوده شدن سیستم به باج‌افزارها و ایجاد مصونیت در برابر از دست رفتن فایل ها و اقدامات واکنشی به منظور بازیابی فایل‌ها پس از آلوده شدن سیستم انجام می‌پذیرد.



اقدامات پیشگیرانه

مرتباً از فایل های خود پشتیبان تهیه کنید: یکی از راه های مناسب برای پیشگیری از خسارات حملات باج افزاری، پشتیبان گرفتن از فایل ها و نگهداری آن ها در جایی غیر از کامپیوترتان است. به این روش، حتی اگر کامپیوترتان به باج افزار آلوده گردد، یک نسخه آلوده نشده از فایل های خود را در اختیار دارید. توجه به این نکته ضروری است که به هیچ وجه نباید از طریق سیستمی که آلوده به باج افزار شده است، فایل های غیر آلوده را باز کرد.

در باز کردن سایت ها و ایمیل های دریافتی، بیش از پیش دقت کنید: از کلیک و یا دانلود و باز کردن ضمیمه ایمیل از افراد ناشناس و یا شرکت هایی که ارتباطی با آن ها ندارید، خودداری نمایید از مشاهده و مرور وب سایت های مشکوک پرهیز کنید.

آنتی ویروس رایانه خود را به روز نگه دارید: نرم افزار آنتی ویروس سیستم خود را همواره به روز نگه دارید. برخی از نسخه های آنتی ویروس ها، قابلیت ضد بدافزار نیز دارند که برای کشف و متوقف کردن بدافزارهای شناخته شده مفید هستند اما امکان مسدودسازی همه برنامه های مخرب را ندارد.

سیستم عامل و سایر برنامه های خود را به روز نگه دارید: هر چه نرم افزارهای نصب شده بر روی سیستم شما به روزتر باشند، نقاط آسیب‌پذیر شناخته شده کمتری دارد و آلوده کردنش برای مجرمان سایبری سخت‌تر است. بنابراین، حتما سیستم‌عامل، اپلیکیشن‌ها و دستگاه‌هایتان قادر به نصب خودکار به‌روزرسانی‌ها باشند. به طور مثال، برای به‌روزرسانی سیستم‌عامل ویندوز ۱۰ می‌توانید به آدرس زیر مراجعه کنید:

https://support.microsoft.com/en-update-10-windows/4027667/ca/help

مشاهده پسوند فایل ها: گزینه مشاهده پسوند فایل ها را در سیستم عامل ویندوز فعال کنید و به پسوند فایل هایی که بر روی آن کلیک می کنید، دقت نمائید.

اقدامات واکنشی

درصورت آلوده شدن به باج‌افزار بایستی توجه شود که در اغلب موارد امکان رمزگشایی فایل‌های رمز شده وجود ندارد. با این اوصاف، توصیه می‌شود در صورت مواجهه با باج‌افزار موارد ذیل رعایت گردد:

- سیستم آلوده را از تمامی شبکه‌ها قطع کنید و کلیه دستگاه‌های ذخیره‌سازی متصل به سیستم را جدا نمائید.
- در صورت امکان سیستم را خاموش نموده و از روشن کردن مجدد آن خودداری نمایید.
- به هیچ وجه فایل‌های رمز شده حذف نگردد. چرا که ممکن است در آینده روشی برای رمزگشایی این فایل‌ها (بدون پرداخت باج) فراهم گردد.
- در صورت اتصال رسانه‌های ذخیره‌سازی پشتیبان (Backup Storage) به سیستم‌های آلوده، فوراً جدا شوند.
- در اغلب موارد پرداخت‌کنندگان باج نیز به دلایل مختلف قادر به رمزگشایی فایل‌های خود نبوده‌اند. از این‌رو توصیه می‌شود از پرداخت باج خودداری گردد.
- در برخی موارد ممکن است در اثر ضعف باج‌افزار در امحا نمودن نسخه اصلی فایل‌ها، امکان بازیابی بعضی از فایل‌های حذف شده با استفاده از ابزارهای File Recovery میسر باشد.
- در موارد محدودی نیز ممکن است به دلیل ضعف باج‌افزار در پیاده‌سازی عملیات رمزنگاری، ابزارهایی برای رمزگشایی فایل‌های رمز شده توسط این باج‌افزار ارائه گردد.

کلیدی ترین اقدام محافظت در برابر باج افزارها:

همواره به طور منظم حداقل ۲ نسخه کپی از داده های مهم خود را در دو محل مجزای دیگر ذخیره نمائید.

توصیه های امنیتی ما را جدی بگیرید!

مرکز نظارت بر امنیت اطلاعات بازار سرمایه

مرکز نظارت بر امنیت اطلاعات بازار سرمایه

تهران، میدان ونک، ابتدای ملاصدرا، شمـاره ۱۳، سازمان بورس و اوراق بهادار
صنـدوق پستـی: ۶۳۶۶-۱۹۹۳۵
تلفن: ۸۴۰۸۳۵۳۵-۰۲۱ makna@seo.ir

www.seo.ir