باج افزار (Ransomware) چیست؟

باج افزار یک بدافزار است که داده های شما را رمزگذاری می کند. یک کلید خصوصی و محافظت شده می تواند فایل های شما را یکبار دیگر قابل خواندن کند. اما هکرها معمولاً آن کلید را به شما نمی دهند مگر اینکه در ازای آن چیزی به آنها بدهید.

حمله باج افزار همیشه جدی است و برخی از سازمان ها آماده هستند تا هر چیزی را برای بازگرداندن پرونده های خود بپردازند. اما شما می‌توانید راه آسیب پذیری هایی که شما را در معرض حمله باج افزار قرار می‌دهند را بسته و در صورتی که هک شده باشید اقدامات فوری برای بازگردانی به وضعیت عادی انجام دهید.

باج افزار چیست؟

شما بارها و بارها کلیک می کنید اما نمی توانید فایل های خود را ببینید. در عوض یک پیام تهدید آمیز می بینید که از شما درخواست پول می کند !چه اتفاقی افتاده است؟ احتمالا با یک باج افزار سر و کار دارید.

برای اجرای حمله، هکرها نرم افزارهای مخرب را در سیستم شما نصب می کنند. تنها چیزی که شما خواهید دید پیام تقاضای پول است. باید هزینه را بپردازید تا دوباره به فایل های خود دسترسی داشته باشید.

باج افزار ممکن است شامل موارد زیر باشد:

یک صفحه تاریک

شما روی پرونده های خود کلیک می کنید و همه چیز سیاه می شود. تنها چیزی که می بینید تقاضای پول یا مجموعه ای از دستورالعمل ها است.

پاپ آپ های بی پایان

دستگاه شما مملو از پنجره های حاوی پیام ، فیلم یا محتواهای غیر اخلاقی است.

خرابی دستگاه ها

برخی از دستگاه ها اصلاً روشن نمی شوند، یا صداهای وحشتناکی ایجاد می کنند که نمی توانید جلوی آنها را بگیرید.

اولین حمله باج افزار مستند در سال ۱۹۸۹ اتفاق افتاد و در سال ۲۰۱۲ بسیار متداول شد. تا این مرحله ، میلیون ها نفر با چنین حمله ای روبرو شده اند.

حمله باج افزار چگونه کار می کند؟

هکرها باهوش هستند و ترفندهای مختلفی دارند که می توانند علیه شما استفاده کنند. حملات باج افزار ناشی از فعالیت های معمولی و روزمره ای است که ممکن است هرگز به آنها مشکوک نباشید یا در مورد آنها دوباره فکر نکنید.

باج افزارها معمولاً از طریق یکی از دو روش زیر (یا هردو) راه اندازی می شوند:

- استقرار دستی .در اینجا ، یک هکر دسترسی اداری به یک سیستم پیدا می کند و باج افزار را در سیستم های هدف قرار می دهد.
- استقرار خودکار .یک سیستم به خطر می افتد و باج افزار از طریق سیستم نصب می شود.

سرورهای شما ممکن است از طریق موارد زیر آلوده شوند:

پاپ آپ ها

در حال بازدید از یک وب سایت هستید و صفحه ای را مشاهده می کنید که به شما اطلاع می دهد به ویروس آلوده شده اید. پیام میگوید روی یک دکمه کلیک کنید تا تهدید را از بین ببرید.

پیام های ایمیل

یک یادداشت برای شما از طریق ایمیل ارسال می شود که می گوید پولی برنده شده اید یا باید دریافت یک محصول را تایید کنید. دکمه ای برای کلیک به شما نشان داده می شود.

فیشینگ

وب سایتی که اغلب از آن دیدن می کنید هک می شود. در حالی که شرایط بسیار شبیه به بازدیدهای قبلی شما است ضربه زدن روی دکمه ها منجر به رفتارهای غیر منتظره می شود.

هنگامی که با وسوسه های تعیین شده توسط هکر درگیر می شوید، کلیک کردن شما منجر به نصب بدافزار می شود. ممکن است متوجه نشوید که این اتفاق می افتد، اما رایانه شما دوست جدیدی پیدا می کند که به سرعت همه پرونده های شما را رمزگذاری کرده و در نتیجه شما نمی توانید به آنها دسترسی پیدا کنید.

وقتی برنامه کامل شد، پیام تقاضای پول به شما نشان داده می شود. مبالغ باج متفاوت است اما اکثر هکرها از افراد مقدار کمی درخواست می کنند. ممکن است از شما ۴۰۰ دلار بخواهند تا پرونده های خود را پس بگیرید.

شرکت های بزرگ با پرونده های فراوان تقاضای پولی بسیار بیشتری را مشاهده می کنند. مواجه شدن با درخواست های هزاران دلاری غیر معمول نیست و ممکن است هکر از شما بخواهد با بیت کوین هزینه را پرداخت کنید.

بازیابی و حذف باج افزار

به سادگی می توان حملات باج افزار را تلاش های ساده ای برای اخاذی دانست. متأسفانه اکثر هکرها از ابزارهای پیچیده ای استفاده می کنند که تکرار یا شکست آنها تقریباً غیرممکن است.

اگر مورد حمله قرار گرفتید ،کارشناسان این مراحل را توصیه می کنند:

۱. راه اندازی مجدد .(Restart) هنگام راه اندازی مجدد از حالت ایمن ویندوز استفاده کنید.
۲. اسکن.(Scan) بر روی هر برنامه آنتی ویروسی که دارید کلیک کرده و تا جایی که ممکن است تست ها و عملکردهای پاکسازی را اجرا کنید.
۳. بازگردانی .(Restore) اگر هنوز نمی توانید به فایل ها دسترسی پیدا کنید ، موارد را به آخرین نسخه ذخیره شده خود برگردانید.

اگر بدافزار از سرور سرچشمه بگیرد، هر گامی که فرد بر می دارد کمکی نمی کند. اگر سیستم کل شرکت شما خراب شده است، تیم فناوری اطلاعات باید برای حل مشکل وارد عمل شود. در حالی که تیم فناوری اطلاعات ویروس ها را پاک می کند و پرونده ها را بازیابی می کند همه کاربران باید از سیستم خارج شوند.

آیا شما می توانید هدف حمله باج افزار باشید؟

هر کسی که دارای یک کامپیوتر کاربردی و مجموعه ای از فایل ها باشد می تواند هدفی برای هکرها باشد. ممکن است فکر کنید چیزی برای به اشتراک گذاشتن ندارید، اما یک هکر خواستار پول شما است. با این حال تعداد زیادی از هکرها منحصراً بر روی اهداف بزرگ از جمله شرکت ها و سازمان های بزرگ تمرکز می کنند.

هکرها می توانند بر سازمان هایی تمرکز کنند که دارای موارد زیر هستند:

- فایل های حساس .سازمان های مراقبت های بهداشتی و درمانی باید پرونده ها را ایمن نگه دارند در غیر اینصورت اعتبار خود را در معرض خطر قرار می دهند. باج افزار می تواند آینده کل سازمان را در معرض خطر قرار دهد.
- تقاضای قابل توجه .سازمانهای دولتی و سایر سازمانهای مشابه برای کارکردن به دسترسی شبانه روزی نیاز دارند. باج در این محیط می تواند به سرعت پرداخت شود.
- اطلاعات به خطر افتاده .سازمان های مالی و شرکت های امنیتی، اطلاعات زیادی در مورد مشتریان خود دارند. حفاظت از داده ها در اینجا می تواند برای ایمن ماندن در تجارت بسیار مهم باشد.

تحلیلگران پیش بینی می کنند که در آینده می توانیم وارد موج جدیدی از حملات باج افزار شویم. هکرها می توانند یک ابزار ساده (مانند یک ایمیل جهانی) بسازند و صدها یا هزاران قربانی را به طور همزمان جذب کنند. شرکت های بزرگ بیش از ۱ میلیارد دلار برای بازیابی اطلاعات پرداخت خواهند کرد.

در گذشته نیز بسیاری از شرکت ها قربانی شده اند. در سال ۲۰۱۷ ، در یکی از بدنام ترین حملات باج افزار ، بیش از ۲۰۰،۰۰۰ کامپیوتر در بیش از ۱۵۰ کشور جهان با اشکال باج افزار WannaCry مورد حمله قرار گرفتند. هکرها پول زیادی به دست آوردند و بسیاری از شرکت هایی که باج پرداخت نکردند فایل های خود را از دست دادند.

چگونه حمله باج افزار را مدیریت کنیم؟

اگر وسوسه شده اید که برای پس گرفتن پرونده های خود به هکرها پول بدهید، تنها نیستید. اما نهادهای دولتی این روش را توصیه نمی کنند. پرداخت های شما هکرها را تشویق می کند تا دیگران را نیز در آینده هدف قرار دهند. همچنین بسیاری از مهاجمان وقتی متوجه می شوند که سازمانی مایل به پرداخت باج است، درخواست پول بیشتری می کنند.

در عوض ، کارشناسان برنامه بهبودی چهار مرحله ای زیر را توصیه می کنند.

۱. گزارش .(Report) این موضوع را به نهاد قانونی مربوطه اطلاع دهید. حملات باج افزاری یک رویداد جنایتکارانه است و مقامات باید در صورت لزوم وارد عمل شوند.
۲. پاک کردن .(Clean up) از یک مشاور مجرب بخواهید تا به شما در بازیابی پرونده های شما کمک کند.
۳. فاز عقب .(Phase back) با پیشرفت کار ، سیستمهای آلوده را به سطح عملکرد عادی خود بازگردانید.
۴. برقراری ارتباط .(Communicate) با هر کداماز شرکای تجاری خود که ممکن است به عنوان بخشی از حمله آلوده شده باشند تماس بگیرید.

هر شرکتی زمانبندی بازیابی متفاوتی دارد. ممکن است فایل های شما پاک شوند، بدافزارها حذف شوند و سیستم ها فقط در عرض چند روز کار کنند. برای سایر شرکتها ،این کار ممکن است ماهها یا حتی سالها طول بکشد.

پیش از شروع اجرای باج افزار از آن جلوگیری کنید!

پاکسازی پس از حمله چندان آسان نیست و ممکن است برخی از فایل ها و داده های خود را برای همیشه از دست بدهید. بنابراین پیشگیری، استراتژی بهتری است، زیرا می توانید مهاجمان را قبل از شروع حمله متوقف کنید.

آژانس امنیت سایبری و زیرساخت های امنیتی دارای یک دفترچه راهنمای ۱۶ صفحه ای حاوی دستورالعمل هایی برای شرکت هایی است که میخواهند امنیت سیستم های خود را تقویت کرده و از حمله بعدی جلوگیری کنند. اکثر این نکات مربوط به نرم افزار است.

نرم افزار نباید استاتیک باشد. شرکت ها وصله هایی را برای کاهش آسیب پذیری ها و جلوگیری از تلاش های هک منتشر می کنند، اما اگر آنها را اعمال نکنید، کمکی نمی کنند. اطمینان حاصل کنید که همیشه در حال بررسی همه دارایی های سازمان خود هستید و قوانین به روز رسانی را اعمال می کنید.

کار شما فنی است، اما مسدود کردن حمله همچنین می تواند شامل اقدامات عاقلانه ای باشد که همه اعضای سازمان شما باید انجام دهند. با کارکنان خود جلسات آموزشی برگزار کنید و در مورد موارد زیر صحبت کنید:

- بهترین محافظت های ایمیل :به تیم خود یادآوری کنید که از کلیک بر روی پیوندهای جاسازی شده در ایمیل خودداری کنند، به ویژه اگر یادداشت ها از شخص دیگری خارج از سازمان آمده باشد.
- حریم خصوصی :بر اهمیت مخفی نگه داشتن نام کاربری و رمزهای عبور تأکید کنید.
- نرم افزار :تاکید کنید که اسکنرهای آنتی ویروس کل شرکت را ایمن نگه می دارند و این سیستم ها باید مجاز به انجام کارهای خود باشند.
- پشتیبان گیری :در صورت هک شدن، بازگشت به نسخه های ذخیره شده ممکن است در وقت و دردسر بیشتر شما صرفه جویی کنند. تیم خود را تشویق کنید تا شیوه های بایگانی را با دقت دنبال کند.

اگر تیم شما تهدیدهایی را که با آنها روبرو می شوید درک کند، ممکن است چشم ها و گوش های بیشتری برای مراقبت از حمله داشته باشید. اگر متوجه مشکلی شدند، می توانید قبل از گسترش آن را متوقف کنید.