آناتومی حمله باج افزارهای رمزنگار

گونه‌های جدید باج افزارهای CryptoDefense، CryptoLocker و CryptoWall از طریق ایمیل‌های هرزنامه، سایت‌های مخرب و یا بدافزارهایی که بر روی سیستم شما هستند منتشر می‌شوند. بمحض آلوده شدن، این باج افزارها با رمزنگاری غیر قابل شکستن، فایل‌های شما را به گروگان گرفته و برای بازگرداندن آنها به حالت قبل ۳۰۰ تا ۵۰۰ دلار اخاذی می‌کنند.

راه‌های پیشگیری و مقابله

- آموزش کاربران
- نصب آخرین اصلاحیه های امنیتی
- بکارگیری ابزارهای پیشگیری از نفوذ
- محدود کردن سطح دسترسی کاربران
- استفاده از دیواره آتش در درگاه شبکه
- تهیه پشتیبان از داده های بااهمیت بصورت دوره‌ای
- استفاده از ضدویروس قدرتمند و به روزرسانی مداوم آن
- بهره‌گیری از نرم افزارها و سخت افزارهای ضدهرزنامه

راه‌های مقابله با باج‌افزارها

ظهور بیش از ۹ باج افزار جدید در هر دقیقه

استفاده از ضدویروس قدرتمند و به‌روز

اصلی‌ترین راه مقابله با باج‌افزارها بکارگیری ضدویروسی با قابلیت‌های شناسایی و حفاظتی قدرتمند و به‌روزرسانی مستمر آن است.

تهیه نسخه پشتیبان بصورت دوره‌ای

تنها راه برای اطمینان از بازگرداندن فوری اطلاعات در صورت آلوده شدن دستگاه به باج‌افزار، وجود نسخه پشتیبان است.

پیروی از قاعده ۳-۲-۱ برای داده‌های حیاتی توصیه می‌شود. برطبق این قاعده، از هر فایل سه نسخه می‌بایست نگهداری شود (یکی اصلی و دو نسخه بعنوان پشتیبان). فایل‌ها باید بر روی دو رسانه ذخیره‌سازی مختلف نگهداری شوند. یک نسخه از فایل‌ها باید در یک موقعیت جغرافیایی متفاوت نگهداری شود.

بهره‌گیری از راهکارهای ضدهرزنامه

هرزنامه‌ها یکی از اصلی‌ترین روش‌های انتشار باج‌افزارها محسوب می‌شوند. استفاده از راهکارهای ضدهرزنامه، بخصوص تجهیزات دیواره آتش به منظور پویش ایمیل‌های دریافتی می‌تواند بطور چشمگیری حجم ورودی هرزنامه‌های ناقل باج‌افزار به سازمان را کاهش دهد.

نصب اصلاحیه های امنیتی

یکی دیگر از روش‌های مورد استفاده باج‌گیران سایبری، سوءاستفاده از ضعف‌های امنیتی سیستم عامل و نرم‌افزارهای رایج همچون Office و Flash است. این افراد می توانند با سوءاستفاده از یک ضعف امنیتی حیاتی بدون نیاز به دخالت کاربر، از راه دور اقدام به نصب باج‌افزار بر روی دستگاه قربانی کنند. شرکت هایی همچون Microsoft و Adobe بطور مستمر اصلاحیه‌های امنیتی برای ترمیم ضعف‌های شناسایی شده در محصولات خود عرضه می‌کنند. استفاده از سرویس‌های WSUS و SCCM به منظور مدیریت توزیع بسته‌ها و اصلاحیه‌های امنیتی در شبکه و همچنین بکارگیری نرم‌افزارهای ضدنفوذ (Host Intrusion Prevention) توصیه می‌شود.

غیرفعال کردن ماکروها

با توجه به انتشار بخش قابل توجهی از باج‌افزارها از طریق فایل‌های نرم‌افزار Office حاوی Macro آلوده، از کار انداختن بخش Macro از طریق فعال نمودن گزینه "Disable all macros without notification" در نرم‌افزار Office برای آن دسته از کاربرانی که به آن نیاز کاری ندارند توصیه می‌شود. مدیران سیستم می‌توانند با بهره‌گیری از تنظیمات Group Policy، اقدام به غیرفعال کردن این قابلیت بصورت متمرکز کنند. همچنین با استفاده از تجهیزات دیواره آتش می‌توان ایمیل‌های دارای پیوست Macro را در درگاه شبکه مسدود کرد.

آموزش کاربران

آموزش و راهنمایی کاربران سازمان به صرف نظر نمودن از ایمیل‌ها و فایل‌های مشکوک و باز نکردن آنها می‌تواند نقشی مؤثر در پیشگیری از آلوده شدن دستگاه ها به باج افزار داشته باشد.

باج‌افزار، تهدیدی پرخطر، مستمر و پیچیده

باج‌افزار: گونه ای بدافزار که دسترسی به فایل‌های کاربر را محدود ساخته و برای دسترسی مجدد، از او درخواست باج می‌کند.

انواع باج‌افزار

رمزنگار پرخطر

باج‌افزار اقدام به رمز کردن فایل‌های کامپیوتر می‌کند.رمزگشایی فایل‌هایی که با طراحی زیرکانه به روش‌های پیشرفته توسط این گونه باج افزار رمزنگاری می‌شوند دشوار و در بسیاری مواقع غیرممکن است.

غیر رمزنگار کم خطر

با نمایش دائمی یک تصویر به نحوی که کاربر قادر به بستن و یا باز کردن پنجره دیگری نباشد، دسترسی کاربر محدود می‌شود.
در تصاویر نمایش داده شده توسط این گونه باج افزار، معمولاً، اینطور القا می‌شود که قفل شدن کامپیوتر توسط نهادهای امنیتی و به دلیل نقض قوانین توسط کاربر، انجام شده است.

باج‌افزارهای رمزنگار سازمان شما را تهدید می‌کنند

استمرار

بر اساس آخرین گزارش شرکت‌امنیتیMcAfee،تعداد باج‌افزارهای جدید در سه ماهه دوم سال ۲۰۱۶، ۱/۳ میلیون عدد بوده است.

داده‌ها

باج‌افزارها می‌توانند داده‌های حیاتی سازمان را رمزنگاری کنند.در بسیاری مواقع رمزگشایی این فایل‌ها بدون پرداخت باج امکان‌پذیر نیست.

خسارت مالی

روزانه بسیاری از سازمان‌ها و شرکت‌ها ناچار به پرداخت باج برای بازگرداندن اطلاعاتشان می شوند.

اعتبار

برخی از گونه‌های جدید باج‌افزارها علاوه‌بر رمزنگاری فایل‌ها، قربانی را تهدید به انتشار فایل‌ها بر روی اینترنت می‌کنند.

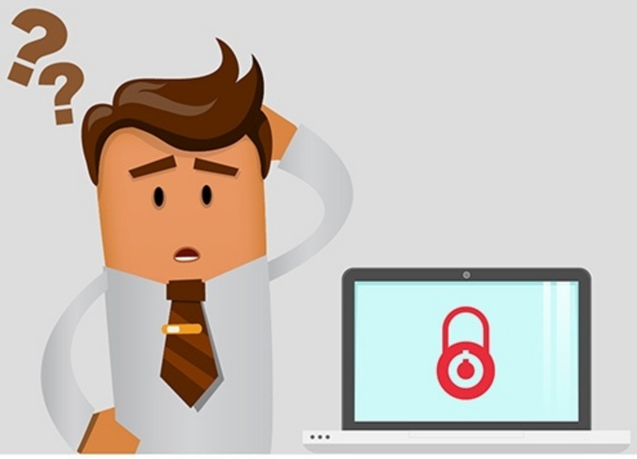
آیا باید باج را پرداخت کنیم؟

نهادهایی همچون FBI قربانیان را تشویق به پرداخت مبلغ باج بعنوان تنها راه بازگرداندن اطلاعات از دست رفته می‌کنند.

ما پرداخت باج را به دلایل زیر توصیه نمی کنیم:

- تضمینی به بازگشت فایل ها به حالت قبل پس از پرداخت باج نیست.
- پرداخت باج عاملی برای استمرار انجام چنین کاری توسط تبهکاران سایبری خواهد بود.

شما آسیب پذیرید اگر...



۱ با تجهیزات از رده خارج کار می‌کنید.	۲ از نرم‌افزار قدیمی استفاده می‌کنید.
٤ راهکار مناسبی برای تهیه پشتیبان ندارید.	۳ فاقد یک استراتژی امنیت سایبری جامع هستید.

۵ سیستم عامل، مرورگر و یا دیگر برنامه‌های کاربردی پراستفاده نصب شده بر روی دستگاه شما فاقد بسته ها و اصلاحیه‌های امنیتی هستند.

پیشگیری، بهترین راهکار

- استفاده از ضدویروس قدرتمند و به روز
- بکارگیری ابزارهای پیشگیری از نفوذ
- نصب آخرین اصلاحیه‌های امنیتی
- تهیه پشتیبان از داده‌های بااهمیت بصورت دوره‌ای
- بهره گیری از نرم‌افزارها و سخت افزارهای ضدهرزنامه
- مسدود کردن ایمیل‌های با پیوست حاوی ماکرو در درگاه شبکه
- محدود کردن سطح دسترسی کاربران
- استفاده از دیواره آتش در درگاه شبکه