باج‌افزارهای رمزگذار

مراحل اخاذی تبهکاران سایبری

باج‌افزارهای رمزگذار یکی از پرطرفدارترین و متأسفانه مخرب‌ترین بدافزارهایی هستند که در چند سال اخیر مورد استفاده تبهکاران سایبری قرار گرفته‌اند. محدود کردن دسترسی به داده‌های حساس از طریق رمزنگاری، ارعاب کاربر و بدنبال آن اخاذی در ازای بازگرداندن این داده‌ها، هدف اصلی این نوع باج‌افزارها است. رمزگشایی فایل‌هایی که با طراحی زیرکانه به این روش رمزنگاری می‌شوند، در بسیاری مواقع غیرممکن است.

۱. توزیع

نفوذ به دستگاه برای اجرای باج‌افزار

هرزنامه

ایمیل‌های با عنوان و محتوای فریبنده که فایل‌های در ظاهر بی‌خطر نظیر ZIP و Office به آنها پیوست شده است. با اجرای پیوست، فایل مخرب بر روی دستگاه اجرا می‌شود. در برخی نمونه‌ها بجای پیوست، از لینک‌های مخرب در درون ایمیل استفاده می‌شود که با کلیک بر روی آن کاربر به یک سایت مخرب هدایت می‌شود.

سوءاستفاده از ضعف‌های امنیتی

وجود یک نقطه ضعف خطرناک در سیستم عامل یا نرم‌افزار نصب شده بر روی دستگاه می‌تواند سبب دور زدن قوی‌ترین نرم‌افزارهای ضدویروس یا دیواره‌های آتش شود! بسیاری از ضعف‌های امنیتی بدون دخالت کاربر قابل بهره‌جویی هستند.

برنامک‌های مخرب

باج‌افزار در برنامک‌های معروف و پراستفاده تزریق شده و در بازارهای توزیع دیجیتال غیررسمی به اشتراک گذاشته می‌شود. با دریافت و نصب برنامک، دستگاه به باج‌افزار آلوده می‌شود.

راهکارهای دفاعی

- آموزش و راهنمایی کاربران سازمان به صرف‌نظر کردن از فایل‌های مشکوک و باز نکردن آنها
- نصب مستمر اصلاحیه‌های امنیتی و ترجیحاً استفاده از نرم‌افزارهای WSUS یا SCCM
- بکارگیری ابزارهای ضدهرزنامه در درگاه شبکه
- استفاده از ابزارهای کنترل وب
- استفاده از ضدویروس قدرتمند و به‌روز
- مسدود کردن ایمیل‌های با پیوست ماکرو

۲. نصب

باج‌افزار خود را بر روی ماشین قربانی نصب کرده و حضور خود را بر روی سیستم ماندگار می‌کند.

راهکارهای دفاعی

- استفاده از نام‌های کابری با سطح دسترسی محدود
- بکارگیری ابزارهای کنترل برنامه برای جلوگیری از اجرای برنامه‌های غیرمجاز

۳. خلع سلاح دستگاه

در برخی نمونه‌های باج‌افزار رمزگذار، تنظیمات امنیتی غیرفعال شده و نسخه‌های کپی شده سیستمی حذف می‌شوند.

حذف Shadow Copy

باج افزار اقدام به حذف نسخه‌های Shadow Copy از طریق پروسه vssadmin.exe برای غیرممکن کردن بازگرداندن فایل‌ها از طریق این قابلیت می‌کند.

حذف System Restore

به‌منظور جلوگیری از بازگشت سیستم به حالت قبل، سوابق System Restore حذف می‌گردد.

راهکارهای دفاعی

- تهیه نسخه‌های پشتیبان؛ پیروی از قاعده ۳-۲-۱ برای داده‌های حیاتی توصیه می‌شود. بر طبق 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 نیز می‌بایست در یک موقعیت جغرافیایی متفاوت نگهداری شود.

۴. اعلام به سرور فرماندهی

با برقراری ارتباط با سرور فرماندهی شناسه‌ای منحصربه‌فرد ایجاد شده و به دستگاه تخصیص داده می‌شود.

راهکارهای دفاعی

- معمولاً باج‌افزارها پیش از برقراری ارتباط با سرور فرماندهی فایل‌های کاربر را رمزگذاری نمی کنند؛ بنابراین استفاده از دیواره آتش و ابزارهای کنترل اینترنت بسیار کمک‌کننده خواهد بود.

۵. به گروگان رفتن داده‌های بااهمیت

رمزگذاری مستندات، تصاویر و به‌طور کلی فایل‌های پراستفاده

رمزگذاری قدرتمند

در باج افزارهای رمزگذار، محدودسازی به دستگاه از طریق رمزگذاری فایل‌های بااهمیت کاربر انجام می‌شود. در این نوع محدودسازی، هدف از رمز کردن، تغییر ساختار فایل است؛ به نحوی که تنها با داشتن کلید رمزگشایی بتوان به محتوای فایل دسترسی پیدا کرد. پیچیدگی و قدرت این کلیدها بر اساس تعداد بیت بکار رفته در ساخت کلید است. هر چه تعداد این بیت‌ها بیشتر باشد شانس یافتن آن هم دشوارتر و در تعداد بیت بالا عملاً غیرممکن می شود.

هدف قرار دادن پسوندهای پراستفاده

بسته به نوع باج‌افزار، فایل‌های با پسوندهای خاص و معمولاً رایج رمزگذاری می‌شوند.

در امان نبودن پوشه‌های اشتراکی و حافظه‌های متصل به دستگاه

علاوه بر فایل‌های موجود بر روی دیسک سخت دستگاه، باج‌افزار پوشه‌های اشتراکی که کاربر دستگاه آلوده شده به آنها دسترسی نوشتن دارد و همچنین حافظه‌های جانبی نظیر حافظه‌های حذف شدنی را نیز هدف قرار می‌دهد.

راهکارهای دفاعی

- تهیه نسخه‌های پشتیبان؛ پیروی از قاعده ۳-۲-۱ برای داده‌های حیاتی توصیه می‌شود. بر طبق 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 می‌بایست در یک موقعیت جغرافیایی متفاوت نگهداری شود.

۶. اخاذی

باج‌افزار پیامی را به قربانی نمایش داده و در آن کاربر در خصوص مبلغ باج و روش پرداخت راهنمایی می‌شود.

پرداخت بیت کوین

اکثر باج افزارها از بیت کوین استفاده می‌کنند. بیت کوین نوعی پول دیجیتال بر پایه اصل اثبات دانایی صفر است. بدان معنا که فرستنده و گیرنده ضمن اطلاع از انتقال پول، از هویت یکدیگر مطلع نمی‌شوند.

پشتیبانی

برخی گردانندگان باج‌افزار دارای سامانه‌هایی برای ارائه خدمات پشتیبانی به قربانیان خود هستند! قربانیان می‌توانند در خصوص مسائلی نظیر نصب Tor خرید بیت کوین از باج‌گیران راهنمایی بگیرند.

رمزگشایی رایگان اما محدود

در برخی باج‌افزارها به قربانی این امکان داده می‌شود تا یک یا چند فایل را به رایگان و به عنوان اثبات توانایی باج‌افزار در رمزگشایی به حالت قبل باز گرداند.

۷. رمزگشایی

هر چند که در اکثر نمونه‌ها با پرداخت باج کار رمزگشایی انجام می‌شود، اما انجام این کار به دلایل مختلف از جمله تشویق تبهکاران سایبری به ادامه این فعالیت‌های مخرب و همچنین عدم وجود تضمینی برای بازگشت فایل‌ها به حالت قبل به هیچ وجه توصیه نمی‌شود.

بهترین راهکار برای مقابله باج افزارهای رمزگذار، پیشگیری از آلوده شدن است.

آیا شما آماده اید؟

کارشناسان شبکه گستر در کنار شما هستند.

شبکه گستر

www.shabakeh.net

۰۲۱ - ۴۲۰۵۲

SPT-A-0127-00