پیروزی در نبرد با باج افزارها

شبکه گستر
شرکت مهندسی شبکه گستر
SPT-A-0107-00

باج افزار یا Ransomware گونه‌ای بدافزار است که دسترسی به فایل‌های کاربر را محدود ساخته و برای دسترسی مجدد، از او درخواست باج می‌کند. در سال‌های اخیر آن دسته از باج افزارهایی که از طریق رمزنگاری اقدام به محدودسازی دسترسی کاربر به فایل‌ها می‌کنند موفقیت‌های بی‌مثالی را نصیب صاحبان تبهکار خود کرده‌اند و بر اساس آمار، تعداد این باج افزارها بشدت در حال افزایش است. در این نوع محدودسازی، هدف از رمز کردن، تغییر ساختار فایل است؛ به‌نحوی 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 می‌شود.

تاریخچه باج افزارها

۱۳۶۸
نخستین باج‌افزار که کامپیوترها را از طریق دیسک فلاپی آلوده می‌کرد شناسایی شد.

۱۳۹۰
باج‌افزار Reveton که با یک اسب تروای بانکی ترکیب شده بود، با قفل کردن دستگاه از طریق نمایش یک تصویر ثابت اینطور القا می‌کرد که مسدود شدن دسترسی به دستگاه توسط نهادهای امنیتی و به‌دلیل نقض قوانین توسط کاربر صورت گرفته و کاربر می‌بایست برای دسترسی مجدد به دستگاه اقدام به پرداخت جریمه - همان باج - کند.

۱۳۹۴
"باج‌افزار به‌عنوان سرویس" (Ransomware-as-a-Service) وارد بازار تبهکاران سایبری شد. سرویسی که تبهکاران بدون دانش برنامه‌نویسی را نیز قادر به استفاده از این نوع بدافزارهای مخرب می‌کند.

۱۳۹۵
تخمین زده می شود که سازنده Cerber سالانه نزدیک به یک میلیون دلار از راه عرضه خدمت "باج‌افزار به‌عنوان سرویس" درآمد داشته باشد.

۱۳۹۵
Mamba، اولین باج‌افزار رمزکننده دیسک سخت، سیستم‌ها را هدف قرار داد.

اصلی ترین اهداف نسل جدید باج‌افزارها

- شرکت‌های کوچک و متوسط
- سازمان‌های دولتی
- مراکز آموزشی
- مراکز درمانی
- مؤسسات مالی و بانکی

آینده باج‌افزارها

هدفمندتر شدن حملات باج‌افزارها

اضافه شدن قابلیت‌های پیشرفته فرار از سد محصولات امنیتی و در نتیجه دشوارتر شدن شناسایی آنها

هدف قرار گرفتن دستگاه‌های همراه و اینترنت اشیاء (IoT) بیش از قبل

نیمی از شرکت‌ها آلوده شدن به باج‌افزار را تجربه کرده‌اند.

برخی سازمان‌ها هر هفته چندین بار به انواع باج‌افزارها آلوده می‌شوند.

در هر دقیقه بیش از ۱۰ باج‌افزار منحصربه‌فرد جدید در جهان منتشر می‌شود.

۲ دلیل برای افزایش شمار باج‌افزارها

۱- جواب می‌دهد! حملات باج‌افزاری اکنون از حملات نشت داده‌ها پیشی گرفته است. دلیل آن اجرای آسان و سودده بودن این حملات برای صاحبان آنها است.

۲- عدم امکان شناسایی باج‌گیران از طریق ردیابی مبالغ پرداختی - با توجه به استفاده آنها از پول‌های مجازی نظیر بیت‌کوین

بازبینه پیشگیری و مقابله با باج افزارها

قبل

آگاهی‌رسانی امنیتی به‌طور مستمر
آموزش صحیح کاربران می‌تواند صدمات ناشی از ایمیل‌های وسوسه کننده مخرب را به‌طور چشمگیری کاهش دهد. کاربرانی که بیش از یک‌بار در طی سال آموزش می‌بینند با احتمال کمتری به دام ترفندهای مهندسی اجتماعی تبهکاران سایبری می‌افتند.

شناسایی آسیب‌پذیری‌ها
آسیب‌پذیری‌ها و نقاط ضعف امنیتی موجود بر روی سیستم‌ها و شبکه سازمان را پیش از آنکه مورد بهره‌جویی مهاجمان قرار گیرند شناسایی و ترمیم کنید.

نصب اصلاحیه‌ها و کنترل سطوح دسترسی
سیستم‌های عامل و نرم‌افزارهای آنها را به‌روز نگاه داشته و سطح دسترسی کاربران به سیستم عامل و پوشه‌های اشتراکی را در کمترین حد ممکن قرار دهید.

استفاده از راهکارهای حفاظتی
با استفاده از راهکارهای ضدویروس، ضدهرزنامه، دیواره آتش، نفوذیاب و کنترل برنامه، بدافزارها و حملات را به‌صورت بلاردنگ شناسایی و مسدود کنید.

تهیه نسخه پشتیبان از سیستم‌ها
از داده‌های بااهمیت به‌صورت دوره‌ای و بنحو صحیح پیشتیبان تهیه کنید.

در حین و بعد

برون خط شوید!
در صورت آلوده شدن دستگاه به باج‌افزار، دستگاه را خاموش کرده و اطمینان یابید دستگاه به شبکه داخلی سازمان و اینترنت دسترسی نداشته باشد. با توجه به زمان‌بر بودن فرآیند رمزنگاری فایل‌ها - البته در اکثر مواقع - خاموش کردن دستگاه ممکن است به نجات برخی از فایل‌ها کمک کند.

بازگردانی اطلاعات
در صورت وجود نسخه پشتیبان از داده‌های رمز شده، دستگاه با دیسک نجات مجهز به ضدویروس به‌روز راه‌اندازی شده و پس از انجام پویش و اطمینان از پاکسازی باج‌افزار داده‌ها بازگردانده شوند.

پویش و حفظ داده‌های رمز شده
در صورت عدم وجود نسخه پشتیبان، دستگاه به همان روش مذکور پاکسازی شود. در نظر داشته باشید که تمامی باج‌افزارها پیچیده نیستند و برخی از آنها تنها باج‌افزارهای رمزنگارنما هستند! بنابراین با پویش شدن ممکن است که اطلاعات در ظاهر رمز شده به حالت قبل بازگردانده شوند. پس از اطمینان از پاکسازی دستگاه فایل‌های رمزشده بر روی حافظه‌ای نگهداری شود.

از پرداخت باج پرهیز کنید
به یاد داشته باشید که حتی در صورت پرداخت باج، تضمینی برای بازگشت فایل‌ها به حالت قبل وجود ندارد.

ردیابی نحوه آلوده شدن دستگاه
نحوه آلوده شدن دستگاه را شناسایی کرده و از تکرار آن جلوگیری کنید.

یک نکته

با توجه به ضبط موردی سرورهای حاوی کلید توسط نهادهای قانونی و اضافه شدن آنها به فهرست به‌روزرسانی ضدویروس‌ها، توصیه می‌شود که این فایل‌ها به صورت دوره ای توسط نرم‌افزارهای ضدویروس به‌روز پویش شوند.

منابع:
- newsroom.shabakeh.net/16262/small-and-medium-sized-businesses-are-main-targets-of-ransomware.html
- newsroom.shabakeh.net/16653/where-is-ransomware-going.html
- newsroom.shabakeh.net/16938/a-hospital-hit-by-random-ransomware-attack.html
- newsroom.shabakeh.net/16948/hollywood-presbyterian-pays-the-ransom.html
- newsroom.shabakeh.net/17607/cerber-as-a-service.html
- newsroom.shabakeh.net/17997/half-of-organizations-have-been-infected-by-ransomware.html
- newsroom.shabakeh.net/18032/nemucod-is-targeting-iranian-users.html
- newsroom.shabakeh.net/18060/mamba-targets-sfmta.html
- securingtomorrow.mcafee.com/mcafee-labs/reveton-ransomware-hides-behind-encryption
- www.checkpoint.com/downloads/resources/cerber-report.pdf
- www.mcafee.com/us/resources/reports/rp-quarterly-threats-sep-2016.pdf
- www.trustwave.com/Resources/Trustwave-Blog/New-Report-on-Phishing-and-Ransomware-Helps-Prepare-You-for-the-Fight

شبکه گستر
شرکت مهندسی شبکه گستر

تلفن / دورنگار ۰۲۱ - ۴۲۰۵۲
رایانامه شرکت info@shabakeh.net
تارنمای شرکت www.shabakeh.net
رسانه تصویری www.shabakeh.net/tv
مرکز آموزش events.shabakeh.net
اتاق خبر newsroom.shabakeh.net