واکنش موثر در برابر باج‌افزارها

درک رفتار باج‌افزارها و نحوه مبارزه موفق با آنها

تاثیر باج‌افزارها در مقایسه با بدافزارهای مخفی‌تری که در حملات پیشرفته مورداستفاده قرار می‌گیرند، فوری است.

درباره باج‌افزار

باج‌افزار یک نوع از بدافزار است که کامپیوتر یا فایل‌های خاصی در سیستم قربانی خود را غیرقابل دسترسی یا غیرقابل استفاده می‌کند. در ادامه نیز در ازای ارائه کلید رمزنگاری که می‌تواند کامپیوتر را به وضعیت قبلی بازیابی کرده یا فایل‌های رمزنگاری‌شده را باز کند از قربانی درخواست باج می‌کند.

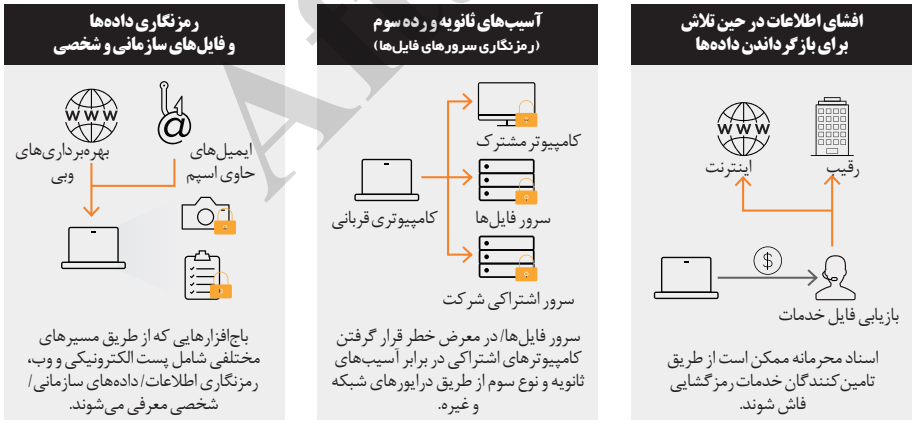
هنگامی که یک سیستم هدف توسط باج‌افزار آلوده شد یک باج‌افزار مدرن، گروهی از فایل‌های حیاتی را هدف قرار داده و رمزنگاری می‌کند تا موجب غیرقابل دسترسی شدن آنها برای کاربر شود، سپس دستورالعمل نحوه پرداخت باج برای بازیابی دسترسی به فایل‌ها را به نمایش می‌گذارد. معمولا واحدهای پول مجازی و آنلاینی مانند پی‌پال یا بیت‌کوین به‌عنوان روش‌های پرداخت معرفی می‌شوند زیرا به‌آسانی قابل‌ردیابی نیستند.

تاثیر باج‌افزارها در مقایسه با بدافزارهای مخفی‌تر مانند مواردی که در حملات و تهدیدهای پیشرفته مورداستفاده قرار می‌گیرند، فوری است. نگرانی درباره اثر پیچیده باج‌افزارها بر روی سازمان‌ها در حال افزایش است که این اثرات شامل ضرر مالی شرکت‌ها در دوران از کارافتادگی سیستم‌شان نیز می‌شود.

آسیب ایجادشده توسط باج‌افزار

سه نوع اصلی آسیب توسط باج‌افزارها ایجاد می‌شوند.

شکل ۱: انواع آسیب ایجادشده به‌وسیله باج‌افزار



رمزنگاری داده‌ها و فایل‌های سازمانی و شخصی

باج‌افزارها، اسناد یا داده‌های مهم را بر روی یک سیستم رمزنگاری می‌کنند تا آنها را برای یک سازمان یا یک فرد مستقل، غیرقابل دسترسی کنند. ازآن‌رو که فایل‌های رمزنگاری‌شده را نمی‌توان با راهکارهای امنیتی موجود در بازار مصرف، بازیابی کرد، قربانی باید یا اقدام به پرداخت باج به هکر کرده و یا از نسخه‌های پشتیبانی که از قبل داشته‌است برای بازیابی داده‌ها استفاده کند. در برخی از موارد محدود می‌توان رخنه‌ای در پیاده‌سازی رمزنگاری باج‌افزار شناسایی کرد و از آن برای بازیابی داده‌ها بهره گرفت. بااین‌وجود بسیاری از خانواده‌های محبوب باج‌افزارها تنها پس از دریافت کلیدهای عمومی یا RSA، از

سرور کنترلی و سرور دستورات هکر، فایل‌ها را رمزنگاری می‌کنند. این امر به این معنا است که مسدود ساختن ترافیک سرور کنترل می‌تواند از رمزنگاری پیشگیری کند.

در بسیاری از مواقع، بازیابی کامل بدون دسترسی به کلید رمزگشایی هکرها، تقریبا غیرممکن است. هنگامی که کامپیوتر به یک باج‌افزار مبتلا شد، آسیب وارده تقریبا همیشه به‌صورت آنی اعمال می‌شود و غیرقابل پرهیز است زیرا داده‌های موجود بر روی کامپیوترها، حداقل به‌صورت موقت، غیرقابل دسترسی خواهندبود.

آسیب‌های نوع دوم و سوم

باج‌افزارها می‌توانند از طریقه‌هایی مانند سرورهای فایل و دستگاه‌های به اشتراک گذاشته‌شده در شبکه، موجب ایجاد آسیب‌های ثانویه و نوع سومی نیز بشوند. اگر کامپیوتر قربانی به چنین دستگاه‌هایی متصل باشد، باج‌افزارها معمولا اقدام به رمزنگاری تمامی منابع به اشتراک گذاشته‌شده خواهند کرد.

یک مجری کمپین‌های مخرب باج‌افزاری می‌تواند باج‌افزار را در طول کمپین خود به سایر قربانیان موجود در سازمان آلوده‌شده نیز انتقال بدهد. ابزارهای محبوب مورداستفاده قرار گرفته برای دانلود باج‌افزار معمولا مجوزهای پست الکترونیکی را نیز به سرقت می‌برند و هکرها از حساب‌های ایمیل فاش شده برای انتشار بیشتر باج‌افزار خود استفاده می‌کنند.

یک کامپیوتر آلوده می‌تواند از طریق این دو روش تکثیر، یک باج‌افزار را به کل یک بنگاه اقتصادی انتقال بدهد و موجب ایجاد آسیب‌هایی چشمگیر شود.

افشای اطلاعات شخصی یا محرمانه در طول تلاش برای بازیابی

مجریان این فعالیت‌های مخرب ممکن است برای سرقت یا سوءاستفاده از داده‌های سیستمی که به باج‌افزار آلوده شده‌است، اقدام کنند. در بسیاری از موارد مشاهده شده‌است که مجریان این تهدیدها، باج‌افزارهای خود را در کنار قابلیت‌های سرقت داده‌ها به اجرا درآورده‌اند. آلودگی با بدافزارهای فعال‌کننده سیستم‌های کلاهبردارانه معمولا به‌عنوان پایگاهی برای اجرای فعالیت‌های یادشده توسط هکر مورد استفاده قرار می‌گیرند.

شدت باج‌افزارها

حجم و گستردگی باج‌افزارها در حال افزایش است و این امر موجب ایجاد آسیب‌هایی بیشتر می‌شود. مهاجمان نیز جری‌تر شده‌اند و تهدید می‌کنند که درصورت عدم پرداخت باج مدنظرشان در زمان مشخص، فایل‌های محرمانه را با آسیب روبه‌رو ساخته یا اینکه آنها را به‌صورت آنلاین منتشر می‌کنند.

FireEye به‌صورت منظم کشف نسخه‌های جدید باج‌افزارها را شناسایی

پنج مثال از گونه‌های مختلف از باج‌افزاری که FireEye شناسایی کرده‌است

CryptoWall- این باج‌افزار که چندماه پس از شناسایی باج‌افزار CryptoLocker پدیدار شد و رفتارهایی مشابه با CryptoLocker را از خود نشان داد. در طول ۶ماه از سال ۲۰۱۴، این باج‌افزار توانست تقریبا یک‌میلیون دلار به‌دست بیاورد.

CTB-Locker- این باج‌افزار که برای نخستین‌بار در سال ۲۰۱۴ کشف شد با استفاده از ویژگی‌هایی مانند کنترل سرور بر پایه Tor و ایجاد آدرس خودکار بیت‌کوین که برای هر قربانی کاملا منحصربه‌فرد بود خود را از همتایانش در آن زمان جدا کرده بود. این باج‌افزار همچنان به مجرمان سایبری فروخته می‌شود.

TorrentLocker- این باج‌افزار پس از نابودی باج‌افزار CryptoLocker ظهور کرد و حتی گفته می‌شود که هر دوی آنها توسط طراحان مشابهی ساخته شده‌اند.

Locky- این باج‌افزار در اوایل سال ۲۰۱۶ شروع به انتشار کرد و از کانال‌های انتشار سطح گسترده مشابهی با بدافزار سرقت گواهی‌نامه Dridex استفاده می‌کند.

TeslaCrypt- این باج‌افزار که ابتدا در فوریه سال ۲۰۱۵ کشف شد، انواع مختلفی از فایل‌ها را که شامل بازی‌های آنلاین می‌شدند رمزنگاری می‌کرد. این بدافزار از تاکتیک‌های متعددی برای کاهش شانس قربانی برای مسدود کردن یا اصلاح آسان آلودگی استفاده می‌کرد. این امر شامل رمزنگاری داده‌ها بدون توجه به اینکه آیا اتصال به سرور کنترل ممکن است یا خیر و پاک کردن نسخه‌های کپی سایه‌ای که می‌توانند برای بازیابی داده‌ها یا سیستم به کار گرفته شوند نیز می‌شد.

Aftaba

و اعلام می‌کند. سیستم هوش امنیتی FireEye، باج‌افزارهایی مانند CryptoWall را که درآمد غیرقانونی یک‌میلیون دلاری در طول دوره ۶ماهه کار خود در سال ۲۰۱۵ به همراه داشت، موردبررسی قرار داده‌است. همچنین FireEye تخمین می‌زند که هکرهای TeslaCrypt در بازه زمانی ۷ فوریه تا ۲۸ آوریل ۲۰۱۵ توانسته‌اند تا رقم ۷۶ هزار و ۵۵۲ دلار به دست بیاورند.

انتظار می‌رود که در طول چند سال آینده، حملات سایبری که از باج‌افزارها استفاده می‌کنند با افزایش روبه‌رو شود. این حملات تقریبا بسیار آسان اجرا می‌شوند و حتی کاربران تازه‌کار کامپیوتر در جهان قادر به اعمال آن هستند.

استراتژی واکنش به باج‌افزار ۱: مکانیزم حمله را شناسایی کنید.

راهکار ساده و تکی برای مبارزه با تهدید رو به افزایش باج‌افزارها وجود ندارد. قربانیان معمولا یا باج مدنظر را پرداخت کرده و امیدوار می‌مانند که مشکل در همان مرحله به پایان برسد یا اینکه خطر قطعی فرایند تجاری خود را با تلاش برای بازیابی به‌صورت شخصی به جان می‌خرند.

پرداخت باج به مهاجمان برای رمزگشایی، یک راه‌حل واقعی نیست. باج دادن به آنها نه‌تنها برای سازمان قربانی، بار مالی به همراه خواهد داشت بلکه به‌صورت مستقیم موجب دریافت پاداش نقدی توسط مهاجم شده و به آنها برای حملات بعدی انگیزه می‌دهد. مقامات و آژانس‌های قانونی به‌هیچ‌عنوان معامله با باج‌گیران را پیشنهاد نمی‌کنند و به‌جای آن بر روی پیشگیری و برنامه‌ریزی برای احتمالات مختلف تاکید دارند.

به‌صورت کلی می‌توان گفت که پیشگیری از آلودگی به باج‌افزارها نیازمند به‌روزرسانی سیستم‌عامل و نرم‌افزارها به آخرین نسخه موجود و اعمال احتیاط لازم برای دسترسی به سایت‌های اخبار، تبلیغات و سایر وب‌سایت‌های دارای نقاط ضعف امنیتی است.

افزایش امنیت ایمیل برای مسدودسازی نامه‌های الکترونیکی ناقل حملات فیشینگ می‌تواند بسیاری از حادثه‌ها را پیش از وقوع متوقف سازد. در شرایط آلودگی، داشتن یک پشتیبانی منظم می‌تواند به کاهش آسیب و شتاب دادن زمان بازیابی کمک شایانی کند.

سازمان‌ها باید تلاش‌های خود را برای شناسایی مکانیزم دقیق نفوذ به کار گرفته شده توسط باج‌افزار تشدید کرده و راهکارهای امنیتی پیشرفته‌ای که می‌توانند از داده‌های حیاتی شرکت در برابر حملات باج‌افزاری دفاع کنند پیاده سازند. یک استراتژی امنیتی مناسب باید به مکانیزم حمله باج‌افزار را به‌صورت کامل تحلیل کرده و معیارهای امنیتی را که می‌توانند میزان آسیب باج‌افزار را کاهش بدهند نیز ارزیابی کند.

باج‌افزارها از دو راه اصلی معرفی می‌شوند: وب و پست الکترونیکی.

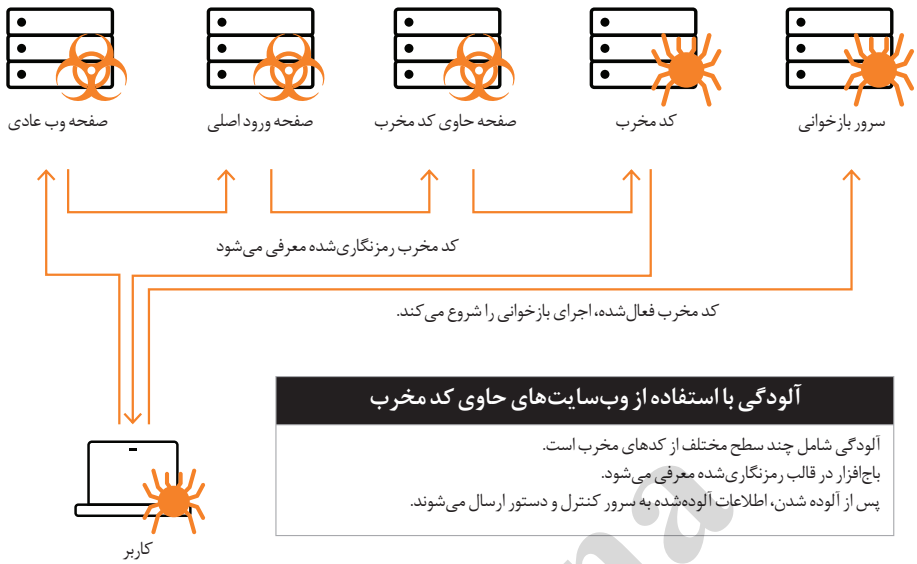
آلودگی از طریق وب

باج‌افزار می‌تواند حمله خود را از طریق وب‌سایت‌های دارای قابلیت بهره‌برداری امنیت صورت بدهند. این امر معمولا با فرایند «اجرا توسط دانلود» به وقوع می‌پیوندد. این فرایند در حقیقت یک کیت بهره‌برداری است که می‌تواند از آسیب‌پذیری‌هایی اصلی که در یک مرورگر وب یا نرم‌افزار وجود دارد، بهره ببرد. مهاجمان یک وب‌سایت قانونی و واقعی را آلوده ساخته یا یک شبکه تبلیغات را هک کرده و کد خود را در آن وارد می‌سازند تا قربانیان را به وب‌سایت دیگر که میزبان یک کیت حاوی کدهای مخرب است، هدایت کند.

کیت‌های حاوی کد مخربی مانند Angler و RI، نرم‌افزارهای آسیب‌پذیری مانند نسخه‌های قدیمی‌تر فلش و جاوا را بر روی سیستم بازدیدکننده شناسایی می‌کنند. آنها می‌توانند بازدیدکننده را به دانلود و اجرای بارکاری مخرب وسوسه کنند. هنگامی که کامپیوتر فرد بازدیدکننده آلوده شد، باج‌افزار به سرورهای کنترل و دستورات متصل شده و به مهاجم اجازه می‌دهد تا بتواند اطلاعات باارزش را به دست بیاورد.

Aftana

شکل ۲: چگونه باج‌افزار، به وسیله وب قربانی می‌کند.



آلودگی با استفاده از وب‌سایت‌های حاوی کد مخرب

آلودگی شامل چند سطح مختلف از کدهای مخرب است.
باج‌افزار در قالب رمزنگاری‌شده معرفی می‌شود.
پس از آلوده شدن، اطلاعات آلوده‌شده به سرور کنترل و دستور ارسال می‌شوند.

در موارد آلودگی بر پایه وب، مسیر دقیق آلودگی را نمی‌توان بدون تحلیل‌های جریان چندمرحله‌ای که کاربر را از یک وب‌سایت ساده به یک منبع توزیع کدهای مخرب راهنمایی می‌کنند، شناسایی کرد. باج‌افزارها می‌توانند به‌دلیل اینکه به‌صورت قالب رمزنگاری‌شده به کامپیوتر فرد قربانی معرفی‌شده‌اند، می‌توانند بدون شناسایی شدن توسط نرم‌افزارهای امنیتی عادی به کار خود ادامه بدهند.

برای شناسایی کدهای رمزنگاری‌شده مخرب به تحلیل رفتار محور نیاز خواهدبود.

برای به حداقل‌رسانی آسیب، ارتباط با سرور کنترل و دستورات باید مسدود شوند تا کدهای مخرب بیشتری دریافت نشده و اطلاعات مهم به خارج ارسال نشوند.

چهار مورد از فعالیت‌هایی که می‌توانند به کاهش آسیب ایجادشده به‌وسیله باج‌افزارهای معرفی‌شده از طریق وب کمک کنند:

- یک تحلیل کامل بر روی تمامی فرانید آلوده شدن، نخست از وب‌سایت عادی که کاربر به سراغ آن رفته بود تا صفحه تغییر مسیر و وب‌سایت نهایی آلوده‌کننده.
- غیرفعال‌سازی اجرای اسکریپت‌های فعال بر روی مرورگرها
- تحلیل فراتری محور کدهای مخرب برای شناسایی شاخص‌های مخرب و آلوده‌کننده سیستم.
- مسدودسازی دسترسی به سرور کنترل و دستورات

آسیب باج‌افزار می‌تواند درصورتی‌که این چهار فعالیت با موفقیت پیاده‌سازی شده باشند به حداقل برسد.

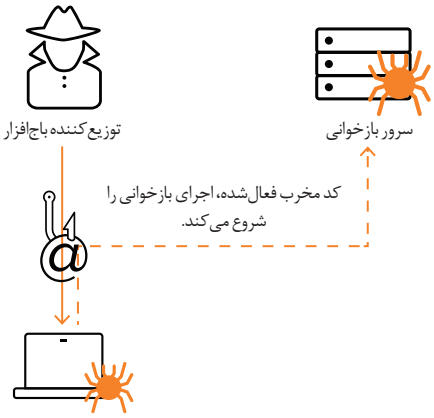
آلودگی از طریق پست الکترونیکی

باج‌افزارها می‌توانند سیستم‌ها را از طریق پست الکترونیکی نیز آلوده سازند. در حقیقت بیشتر موارد آلودگی‌های باج‌افزاری گزارش‌شده از طریق پست الکترونیکی انجام شده‌بودند. بر اساس گزارشی که توسط اتحادیه تهدیدهای امنیتی (CTA) منتشر شده‌است، CryptoWall نسخه ۳ که موجب ایجاد آسیبی ۳۲۵ میلیون دلار در تمامی جهان شده‌است از طریق حمله فیشینگ و به کمک پست الکترونیکی (۶۷٫۳درصد) و کیت مخرب (۳۰٫۷) منتشر شده‌است. در شرایط معرفی از طریق پست الکترونیکی معمولا یک باج‌افزار از طریق یک فایل الحاقی مانند یک فایل فشرده‌شده، فایل‌های حاوی اسناد یا فایل‌های html و یا از طریق لینک

Aftana

موجود در پیام نامه الکترونیکی یا سند الحاقی به سیستم تحویل داده می‌شود. مهاجمان بیشتر از طریقه مهندسی اجتماعی کاربران را مجبور به اجرای فایل یا کلیک کردن بر روی لینک می‌کنند تا اینکه بخواهند از طریق آسیب‌پذیری‌های سیستمی این کار را انجام بدهند. تحلیل رفتار محور، یک روش موثر در برابر باج‌افزارهایی هستند که از طریق پست الکترونیکی منتقل می‌شوند. تحلیل رفتاری موجب می‌شود تا بتوان راه‌های حمله را به‌صورت فعالانه مسدود ساخته و میزان آسیب و یا آلودگی را به حداقل رساند.

شکل ۳: باج‌افزارها چگونه از طریق پست الکترونیکی قربانیان خود را آلوده می‌کنند.



آلودگی از طریق نامه الکترونیکی

تلاش برای آلوده سازی از طریق فایل‌های الحاقی، لینک‌های مخرب و غیره.
تلاش برای آلوده سازی از طریق انواع مختلف فایل
مجبور کردن کاربر برای فعال‌سازی کدها از طریق فنون مهندسی اجتماعی

استراتژی واکنش به باج‌افزار. ۲. پیاده‌سازی راهکارهای پیشرفته امنیتی

بنگاه‌های امنیتی به‌سرعت راهکارهای طراحی‌شده برای مبارزه با تاثیر رو به افزایش باج‌افزارها را طراحی می‌کنند. بااین‌وجود بسیاری از بهترین راهکارها بر روی تهیه نسخه پشتیبانی از فایل‌ها و یا شناسایی رویه‌های خاص باج‌افزاری تمرکز دارند. این موارد به‌صورت کلی اطلاعات واضحی را درباره اینکه حمله چگونه راه خود را به کامپیوتر هدف پیدا کرده‌است و یا اینکه چگونه می‌توان به‌صورت موثر حملات را مسدود ساخت، ارائه نمی‌کنند.

راهکار امنیتی FireEye فرایند حملات باج‌افزاری را به‌صورت شفاف ارائه می‌کند. آنها برای واکنش موثر، یک استراتژی امنیتی بر پایه روش نفوذ باج‌افزار (وب یا پست الکترونیکی) ارائه می‌کنند.

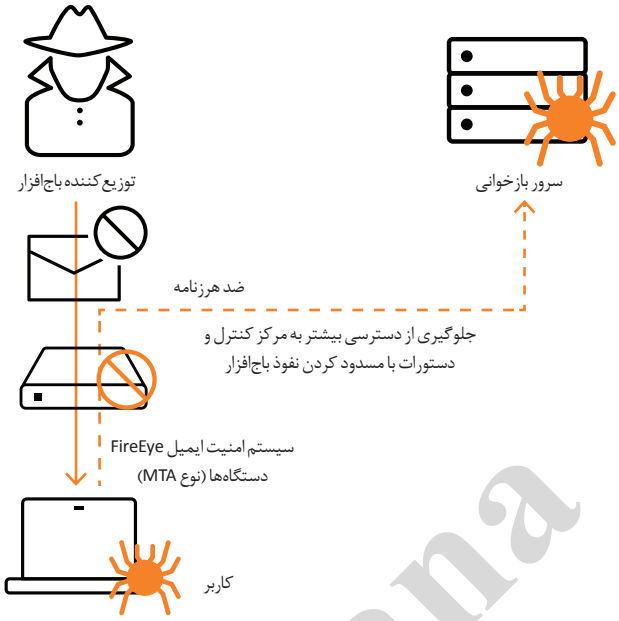
امنیت پست الکترونیکی، نخستین خط دفاع است

یک راهکار امنیت پست الکترونیکی، باج‌افزارهایی را که از طریق ضمیمه‌های موجود در نامه‌های الکترونیکی یا لینک‌های مخرب مخفی انجام می‌شوند، شناسایی و مسدود می‌کند.

بخش عمده‌ای از باج‌افزارها با استفاده از پست الکترونیکی به‌عنوان ابزار ورودی، به یک سازمان وارد می‌شوند که این نام الکترونیکی معمولا از نوع حملات فیشینگ مدل spear phishing هستند. spear phishing یکی از استراتژی‌های ترجیحی در حمله است زیرا شناسایی آن دشوار است. تکیه داشتن این حمله بر روی مهندسی اجتماعی موجب می‌شود تا نرخ موفقیت آن بالا باشد و حتی می‌تواند متخصصان امنیتی و مدیران فناوری سطح بالا را نیز فریب بدهد. تنها چیزی که برای این کار موردنیاز است، یک نامه الکترونیکی برای فعال‌سازی باج‌افزار و قفل کردن دارایی‌های باارزش است.

سیستم امنیت ایمیل FireEye می‌توان این نامه‌های الکترونیکی مخرب را از طریق اجرا کردن و تحلیل فایل مشکوک الحاقی یا آدرس لینک داخلی، مسدود کند. سیستم امنیت ایمیل FireEye می‌تواند یا در محیط‌هایی که با سری EX سازگاری دارند و یا از طریق ارتباط ابری با سیستم ابری حفاظت پست الکترونیکی (ETP) اجرا شود. هنگامی که راهکار امنیت ایمیل FireEye به‌صورت موازی با ساختار ترافیکی SMTP پیاده‌سازی می‌شود، می‌تواند به‌صورت خودکار به شناسایی و مسدود کردن باج‌افزارها دست‌زده و این کار را پیش از آنکه بتوانند به‌سوی کاربر نهایی رخنه کنند، انجام بدهد و به‌این‌ترتیب از رمزنگاری مخرب داده‌ها پیشگیری کند. (شکل ۴)

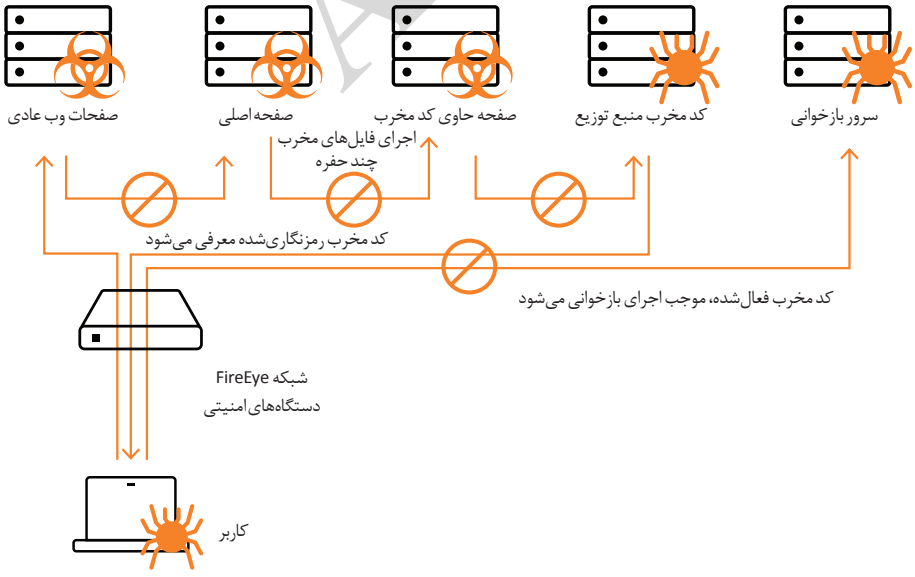
شکل ۴: سیستم امنیت ایمیل FireEye چگونه می‌تواند حملات باج‌افزاری را شنایی و مسدود کند



امنیت شبکه، توزیع را متوقف می‌سازد

یک راهکار امنیتی شـــبکه، مســـیر توزیع و آلوده‌سازی باج‌افزار را شناسایی کرده و باج‌افزار را برای به حداقل رساندن آسیب، مسدود می‌کند.

شکل ۵: سیستم امنیت شبکه FireEye چگونه حملات باج‌افزاری بر پایه وب را شناسایی و مسدود می‌کند.



Afana

می‌توان از طریق شناسایی دقیق سایت‌های توزیع‌کننده و منتشرکننده باج‌افزار و مسدود کردن آنها از حملات باج‌افزاری بر پایه وب پیشگیری کرد. (شکل ۵)

نفوذ باج‌افزار شامل سه مرحله اصلی است: آلودگی اولیه، رمزنگاری داده‌ها و دسترسی به سرور کنترل و دستورات

حمله اولیه

در این مرحله قربانی از یک وب‌سایت عادی به یک سایت انتشاردهنده کدهای مخرب انتقال پیداکرده و سپس فایل‌های حاوی کدهای مخرب اجرا می‌شوند. باید برای شناسایی و مسدود کردن سایت‌های توزیع، جریان کلی شبکه را تحلیل کرد. راهکار امنیتی شبکه FireEye می‌تواند فرایند اقدام برای حمله از طریق ترافیک شبکه را شناسایی کند. این امر به سازمان‌ها اجازه می‌دهد تا بدانند که کدام وب‌سایت‌ها به‌عنوان سایت‌های توزیع باج‌افزار مورداستفاده قرار می‌گیرند و یک سیاست مسدودسازی فعال برای آنها را اعمال کنند.

در یک مورد که اخیرا رخ داده‌است، کاربری که به‌دنبال کلمه کلیدی Park Byeong-hoposting بوده‌است تا به تعدادی از صفحات خبری و پرتال‌های کره‌ای‌زبان دسترسی پیدا کند به یک وب‌سایت حاوی کد مخرب انتقال پیدا کرد و در آنجا کامپیوتر او به باج‌افزار آلوده شد. مشتریانی که از راهکار امنیتی FireEye استفاده می‌کنند، به‌خوبی تلاش‌های اولیه برای آلوده‌سازی را شناسایی می‌کنند. جریان کاری FireEye از طریق ارائه پیشنهادها و اعمال فعالیت‌های زیر انجام می‌شود. نخست مشتریان آدرس صفحات پیاده‌سازی کدهای مخرب و سایت‌های اخبار آنلاین را مسدود می‌سازند، البته درصورتی که با کسب‌وکار آنها ارتباطی نداشته باشد.

این امر می‌تواند از دسترسی به میزبانی که توسط باج‌افزارها مورداستفاده قرارگرفته است، پیشگیری کند. FireEye شاخص‌های در معرض خطر قرار داشتن (IOC) درزمینه باج‌افزارها را جمع‌بندی کرده و با مشتریان خودو به اشتراک می‌گذارد تا بتواند روش‌های جدید احتمالی درخطر قرار گرفتن را موردبررسی قرار بدهد. درنهایت نیز برای جلوگیری از فعالیت‌ها و رخنه‌های مخرب تحت وب، شرکت‌های هدف باید فناوری‌های وبی خود (جاوا، فلش، سیلورلایت و غیره) را به آخرین نسخه موجود به‌روزرسانی کنند.

رمزنگاری فایل‌ها

در این مرحله، سیستم آلوده‌شده به باج‌افزار ممکن است شروع به نشان دادن رفتارهای غیرعادی نماید. اگر باج‌افزار بتواند از فرایند شناسایی در طول مراحل اولیه آلوده سازی فرار کند ولی در این مرحله شناسایی شود، راهکار امنیت شبکه FireEye اقدام به انجام یک تحلیل با جزئیات فراوان درزمینه کدهای مخرب کرده و از شاخص‌های در معرض خطر قرار داشتن برای مسدود کردن باج‌افزار استفاده می‌کند. این امر موجب می‌شود تا یک معیار واکنش شکل گرفته و میزبان‌های آلوده، شناسایی شوند.

برای مثال اگر یک باج‌افزار بتواند قابلیت از کار انداختن بخش مزایای بازیابی ویندوز یا فایل‌های رمزنگاری‌شده را داشته باشد، راهکار FireEye به تحلیل این رفتارها پرداخته و جزئیاتی از شاخص ردیابی برای کاربر مهیا می‌سازد. این امر نه‌تنها برای شناسایی مجدد حمله مشابه در برابر سایر کاربران مفید خواهد بود بلکه می‌تواند از انتشار باج‌افزار از طریق سیستم‌های متصل نیز پیشگیری کند.

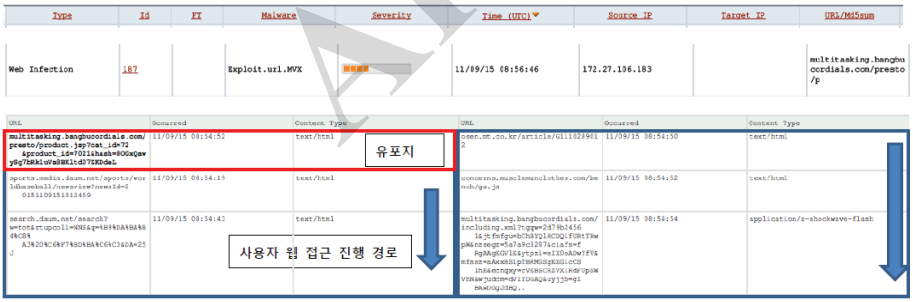
دسترسی به سرور کنترل و دستورات

باج‌افزار در این مرحله اطلاعات آلوده‌شده را به سرور کنترل و دستورات ارسال کرده و یا اینکه مقادیر کد رمزنگاری را از آنها دریافت می‌کند. راهکار امنیت شبکه FireEye، دسترسی به سرور کنترل و دستورات را شناسایی و مسدود می‌کند. اگر یک باج‌افزار نتواند با سرور کنترل و دستورات خود ارتباط برقرار کند، دیگر نخواهد توانست تا داده‌ها را رمزنگاری کرده و یا سایر انواع آسیب را ایجاد کند.

Aftab

شکل ۶: مثال: سیستم امنیت شبکه FireEye چگونه با باج‌افزارهای مبتنی بر وب مبارزه می‌کند

شکل ۷. اطلاعات فرایند اجرای فایل‌های مخرب که توسط مرکز امنیتی FireEye ارائه‌شده‌اند.



نمونه راهکار اجرایی

هسته راهکارهای امنیتی FireEye برای شبکه و پست الکترونیکی، موتور اجرای مجازی چندمحوره (mvx) قرار دارد که فایل‌ها را در محیطی مجازی اجرا و تحلیلی می‌کند. این سیستم در سطحی به‌مراتب فراتر از فناوری سندباکس مرسوم عمل می‌کند.

موتور MVX از یک هایپروایزر اختصاصی و شخصی‌سازی‌شده و انحصاری برای شناسایی و تحلیل چند سطحی کدهای مشکوک در گستره بزرگی از سیستم‌های عامل، نرم‌افزارهای کاربردی، مرورگرها و پلاگین‌ها استفاده می‌کند تا بتواند تهدیدهای سایبری را به‌صورت هم‌زمان شناسایی کرده و مسدود کند. این فناوری

Aftana

حتـــی بـــرای مســـیرها و روش‌های ناشـــناخته یا حمـــلات روز صفر نیز یک تحلیل و مسدودســـازی مفیـــد و تاثیرگذار را تامین می‌کند.

در حقیقت در ژوئن سال ۲۰۱۶، FireEye توانست تا ۲۸ مورد از ۴۸ شناسایی حمله روز صفری را که توسط شرکت‌های امنیتی صورت گرفته بود به خود اختصاص بدهد. موتور MVX با قابل رویت بودن تمامی فرایند مجازی‌سازی در طول چرخه حیات یک حمله باج‌افزاری، از شروع نفوذ تا آلوده سازی، به کاربر اجازه می‌دهد تا بتواند یک واکنش سریع و موثر را از خود ارائه کند. آســـیب‌های ناشـــی از باج‌افزارها به دلیل این‌که شناسایی سایت‌های توزیع‌کننده آن‌ها دشوار است با سرعت زیادی افزایش می‌یابند.

FireEye فنـــاوری خـــود و چنـــد دهه تخصـــص را ترکیب کرده و از آن یک روش قابل‌اعتماد برای شناســـایی ســـایت‌های خطرناک و آسیب‌رســـان ایجاد کرده‌اســـت. به‌این‌ترتیب FireEye به مشـــتریان خود اطلاعاتی موردنیاز را ارائه کرده و از آنها برای شناســـایی هر دو نوع حملات بر پایه وب و بر پایه پســـت الکترونیک که در این ســـایت‌ها مورداســـتفاده قرار می‌گیرند، کمک می‌کند.

جمع‌بندی

تهدید حملات باج‌افزاری از هر زمان دیگری واقعی‌تر به نظر می‌رسد زیرا پیشرفت و تکامل باج‌افزارها همچنان ادامه دارد و در کنار آن نیز باج‌افزارها توانســـته‌اند تا هزینه‌های مالی مســـتقیمی را برای شرکت‌ها به همراه داشته و سیستم کاری آنها را از کار بیندازند.

تولیدکنندگان باج‌افزارها نیز به پیگیری تاکتیک‌های جدید و توسعه انواع نوینی از کدهای مخرب خود ادامه خواهند داد و انواع مختلف و غیرقابل‌شمارش باج‌افزارها نیز معمولا توسط نرم‌افزارهای ضدویروس، شناسایی نمی‌شوند.

هنگامی که ســـازمانی به باج‌افزار آلوده شـــد باید انتظار آســـیب‌هایی جدی را داشته باشد. شناسایی و پیشگیری پیشرفته را می‌توان بهترین دفاع ممکن به‌حســـاب آورد. اگر خودتان و دشـــمن‌تان را بشناســـید آنگاه در مبارزه برتری خواهید داشـــت و ایـــن امر درزمینه امنیت ســـایبری نیز صادق اســـت. برای کاهش شـــانس حمـــلات باج‌افزاری، ســـازمان‌ها باید در طول لایه‌های امنیتی سیســـتم داخلی خود شـــفافیت داشـــته و درکی قـــوی از ابزارها، تاکتیک‌هـــا و روش‌های کاری مهاجمان داشته باشند

منبع: فایر آی