سازمان بورس و اوراق بهادار
SECURITIES & EXCHANGE ORGANIZATION

نکات امنیتی در خصوص پیشگیری و مقابله با باج‌افزارها

مرکز نظارت بر امنیت اطلاعات بازار سرمایه

نسخه ۱,۰

۱۳۹۶/۰۴/۰۴

فهرست

۱- باج‌افزار چیست؟

باج‌افزارها نوع پیچیده‌ای از بدافزارها می‌باشند که دسترسی قربانی را به فایل‌های خود قطع نموده و دسترسی مجدد قربانی به فایل‌ها تنها پس از پرداخت باج میسر خواهد گردید. باج‌افزارها دارای دو نوع مختلف می‌باشند.

باج‌افزارهای رمز کننده، که متداول‌ترین نوع باج‌افزارها می‌باشند، از الگوریتم‌های پیشرفته برای رمزگذاری فایل‌ها و مسدودسازی دسترسی کاربران استفاده نموده و در قبال ارائه کلید رمزگشایی درخواست باج می‌نمایند. به عنوان نمونه می‌توان به CryptoLocker، Locky و CryptoWall اشاره نمود.

باج‌افزارهای قفل کننده، که فایل‌های کاربر را قفل نموده و تا زمان دریافت باج، از دسترسی کاربر به داده‌ها و فایل‌های موجود بر روی سیستم قربانی جلوگیری می‌نماید. شایان ذکر است که این نوع باج‌افزارها، فایل‌ها را رمزگذاری نمی‌نمایند. Winlocker به عنوان نمونه‌ای از این نوع باج‌افزار می‌باشد. برخی از این باج‌افزارها، MBR[۱] را نیز آلوده می‌نمایند. در این صورت فرآیند Boot شدن سیستم به طور صحیح و کامل انجام نپذیرفته و تنها پیغامی مبنی بر درخواست باج نمایش داده می‌شود. باج‌افزارهای Satana و Petya از این دسته باج‌افزارها می‌باشند.

۲- ویژگی‌های کلیدی باج‌افزارها

باج‌افزارها دارای چندین ویژگی کلیدی می‌باشند که آنها را از سایر بدافزارها تمایز می سازد. برخی از این موارد عبارتند از:

- **استفاده از الگوریتم‌های رمزنگاری قوی**: به عبارت دیگر کاربر قادر نیست بدون در اختیار داشتن کلید، اقدام به رمزگشایی فایل‌های رمز شده نماید.
- **توانایی رمزنگاری انواع مختلف فایل‌ها**: باج‌افزارها قادر به رمزگذاری انواع مختلف فایل‌ها شامل اسناد، تصاویر، فایل‌های تصویری، صوتی و غیره می‌باشند.
- **به هم ریختن نام فایل‌ها**: در این صورت، قربانی قادر به شناسایی و تشخیص فایل‌هایی که تحت تاثیر قرار گرفته‌اند، نخواهد بود. این امر یکی از روش‌های مهندسی اجتماعی به منظور مجبور نمودن قربانی به پرداخت باج می‌باشد.
- **افزودن پسوند متفاوت به نام فایل**: این امر به منظور نمایش نژاد باج‌افزار صورت می‌پذیرد.
- **نمایش پیغام یا تصویر**: پیغام یا تصویری با مضمون اطلاع‌رسانی در خصوص رمزگذاری داده‌ها و درخواست باج به قربانی نمایش داده می‌شود.

---

[۱] Master Boot Record

- **درخواست باج به صورت بیت‌کوین:** به دلیل غیرقابل ردیابی بودن بیت‌کوین توسط مراجع قانونی و محققان امنیتی، باج به صورت بیت‌کوین درخواست می‌گردد.
- **دارای مهلت محدود برای پرداخت باج:** در اغلب موارد، به منظور افزایش فشار روانی بر روی قربانی، برای پرداخت باج مهلت زمانی در نظر گرفته می‌شود. پس از پایان این مهلت، مقدار باج افزایش یافته یا دیگر امکان رمزگشایی فایل‌ها میسر نخواهد بود.
- **استفاده از مجموعه روش‌های فرار از آنتی‌ویروس:** باج‌افزارها از تکنیک‌های مختلفی برای ناشناخته ماندن در مقابل آنتی‌ویروس‌های قدیمی استفاده می‌نماید.
- **استفاده از سیستم آلوده شده در بات‌نت‌ها:** در اغلب موارد، مجرمان سایبری سیستم‌های آلوده شده را به منظور گسترش زیرساخت خود جهت انجام حملات بیشتر، در بات‌نت‌ها به کار می‌گیرند.
- **انتشار در سایر سیستم‌های متصل به شبکه محلی:** باج‌افزارها می‌توانند با هدف انجام تخریب و دریافت باج بیشتر اقدام به انتشار در سایر سیستم‌های متصل به شبکه محلی نمایند.
- **قابلیت استخراج داده‌های حساس**: در برخی موارد، علاوه بر رمزگذاری فایل‌ها، باج‌افزار ممکن است داده‌های حساس موجود بر روی سیستم آلوده شده (مانند نام‌های کاربری، کلمات عبور، آدرس‌های ایمیل و غیره) را استخراج نموده و به سرور کنترل کننده خود ارسال نمایند.
- **دارای هدف جغرافیایی خاص**: در برخی مواقع، باج‌افزار دارای اهداف جغرافیایی خاص بوده و حتی برای افزایش شانس پرداخت باج، پیغام‌ها به زبان قربانی ترجمه می‌شوند.

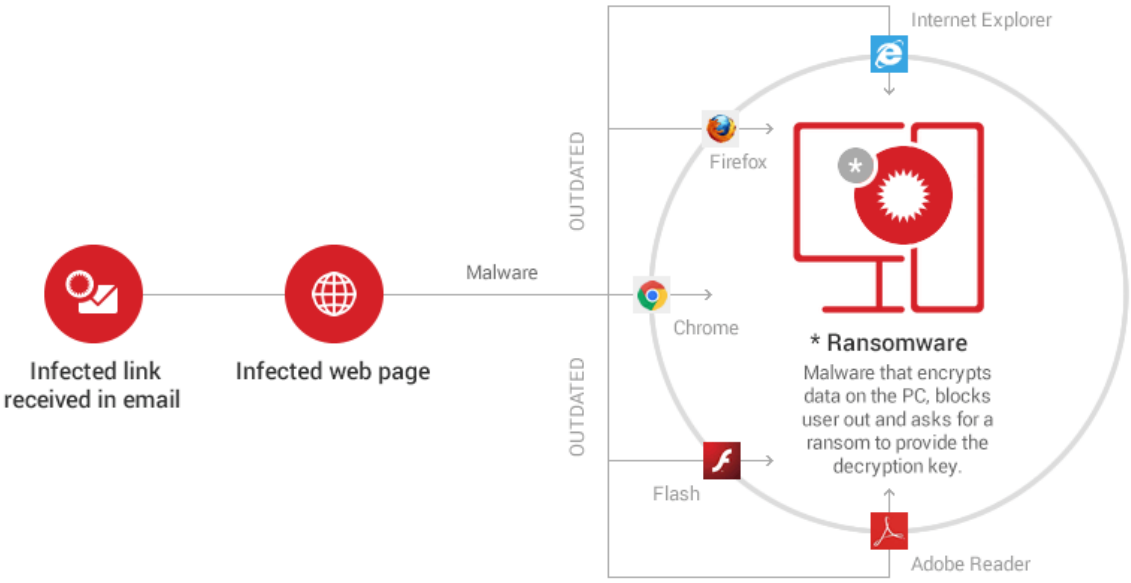
با توجه به رشـــد روز افزون باج‌افزارها و افزودن قابلیتهای جدید به اینگونه بدافزارها، ویژگی‌های فوق‌الذکر در حال افزایش می‌باشند.

۳- نحوه انتشار و آلوده‌سازی باج‌افزارها

مجرمان امنیتی به دنبال ساده‌ترین راه برای آلوده‌سازی سیستم‌ها یا شبکه و استفاده از آن برای انتشار بدافزار می‌باشند. متداول‌ترین روش‌هایی که بدین منظور توسط مجرمان امنیتی مورد استفاده قرار می‌گیرد عبارتند از:

- هرزنامه‌های دارای لینک یا فایل‌های پیوست
- آسیب‌پذیری‌های امنیتی در نرم‌افزارها
- ریدایرکت ترافیک اینترنت به وب‌سایت‌های مخرب
- وب‌سایت‌های مجازی که کدهای مخرب در صفحات آن تزریق شده است
- از طریق تبلیغات اینترنتی
- بات‌نت‌ها
- باج‌افزارهای خودانتشار

علیرغم اینکه فاز آلوده سازی در باجافزارهای مختلف تا حدودی متفاوت می‌باشد، لیکن مراحل اصلی این فاز به شرح ذیل است.



۱) در ابتدا، قربانی یک ایمیل حاوی لینک مخرب یا فایل پیوست (بدافزار) دریافت می‌نماید. همچنین این گام می‌تواند به هریک از روش‌های فوق‌الذکر صورت پذیرد.

۲) در صورتیکه قربانی بر روی لینک مذکور کلیک نموده و یا فایل پیوست را باز نماید، فایل نصب‌کننده بدافزار بر روی سیستم قربانی قرار می‌گیرد.

۳) فایل نصب کننده بدافزار لیستی از دامنه‌ها یا سرورهای C&C[۲] خود را به منظور دانلود برنامه باجافزار بر روی سیستم استفاده می‌نماید.

۴) سرور C&C محتوای درخواستی را به فایل نصب کننده ارسال می‌کند.

۵) باجافزار، کل محتوای دیسک سخت، فایل‌های شخصی و اطلاعات حساس را رمزگذاری می‌نماید. داده‌های ذخیره شده در حساب‌های کاربری ابری (مانند Google Drive و Dropbox) با سیستم تحت تاثیر همگام[۳] می‌گردد. همچنین ممکن است داده‌های مربوط به سایر سیستم‌های متصل به شبکه محلی رمزگذاری شوند.

۶) پیغام هشداری به کاربر نشان داده شده و دستورالعمل پرداخت باج به منظور دریافت کلید رمزگشایی تشریح می‌گردد.

---

[۲] Command and Control

[۳] Sync

۴– نمونه‌هایی از مشهورترین باج‌افزارها

اولین باج‌افزار در سال ۱۹۸۹ با عنوان AIDS Trojan ایجاد گردیده بود که اقدام به مخفی نمودن دایرکتوری‌ها و رمزگذاری اسامی فایل‌های موجود در درایو C: می‌نمود. این باج‌افزار از طریق فلاپی دیسک منتشر می‌شده و ۱۸۹ دلار به عنوان باج درخواست می‌نمود. در ادامه، نمونه‌هایی از مشهورترین باج‌افزارها که اخیرا منتشر شده‌اند معرفی خواهد گردید.

- **WannaCry**: در تاریخ ۱۲ می ۲۰۱۷، حمله باج‌افزاری در سطح بی‌سابقه‌ای شروع به انتشار WannaCry نمود. این باج‌افزار از یک آسیب‌پذیری سیستم‌عامل ویندوز برای انتشار خود استفاده می‌نماید. طی آمارهای منتشر شده حدود ۴۰۰,۰۰۰ سیستم در بیش از ۱۵۰ کشور توسط این بدافزار آلوده شده‌اند.
- **Petya**: خانواده باج‌افزار Petya اولین بار در سال ۲۰۱۶ کشف گردید. این باج‌افزار اقدام به آلوده‌سازی MBR[۴] و رمزگذاری فایل‌های موجود می‌نماید. سپس در ژوئن سال ۲۰۱۷، نسخه دیگری از خانواده باج‌افزار Petya منتشر گردید که قابلیت خودانتشاری در آن بهبود یافته است. این نسخه نیز از آسیب‌پذیری سیستم‌عامل ویندوز برای انتشار خود استفاده می‌نماید.
- **Locky**: بدافزار Locky اولین بار در فوریه ۲۰۱۶ کشف گردید. این نسخه با اخاذی ۱۷۰۰۰ دلار از یک بیمارستان در Hollywood کشف گردید.

[۴] Master Boot Record

- **TorrentLocker**: این باج‌افزار رمز کننده در اوایل سال ۲۰۱۴ ظهور نمود. سازندگان آن اغلب تمایل داشتند از آن با عنوان CryptoLocker یاد نمایند. انتشار باج‌افزار TorrentLocker از طریق هرزنامه‌ها انجام می‌شد. به منظور افزایش کارایی در انتشار، این باج‌افزار مخاطبان جغرافیایی خاصی را در ارسال ایمیل مد نظر قرار می‌داد. محققان بدافزار توانستند برای نسخه اولیه این باج‌افزار ابزار رمزگشایی ایجاد نمایند. از اینرو، سازندگان TorrentLocker نسخه جدیدی را با قابلیت رمزنگاری قویتر ارائه دادند که شانس شکستن آن تقریبا رو به صفر بود.
- **CryptoLocker**: این باج‌افزار در سال ۲۰۱۳ کشف گردید. فعالیت باج‌افزار CryptoLocker در اکتبر سال ۲۰۱۳ با آلوده‌سازی بیش از ۱۵۰،۰۰۰ کامپیوتر در یک ماه به اوج خود رسید.
- **CryptoWall**: باج‌افزار CryptoWall یکی دیگر از باج‌افزارهای مشهور است که نسخه‌های مختلفی از آن منتشر شد که نشان از سرعت بهبود آن دارد. آخرین نسخه این باج‌افزار CryptoWall 4.0 می‌باشد.
- از باج‌افزارهای معروف و مخرب دیگر می‌توان به CTB Locker، Reveton و TeslaCrypt اشاره نمود.

۵- مقابله با باج‌افزارها

مقابله با باج‌افزارها می‌تواند به دو صورت پیشگیرانه و واکنشی مطرح شود. اقدامات پیشگیرانه به منظور جلوگیری از آلوده شدن سیستم به باج‌افزارها و اقدامات واکنشی به منظور بازیابی فایل‌ها پس از آلوده شدن سیستم انجام می‌پذیرد.

۵-۱- اقدامات پیشگیرانه

توجه به این نکته ضروری است که برای مقابله با باج‌افزارها، در اکثر موارد تنها اقدامات پیشگیرانه موثر می‌باشند. مواردی که بایستی تحت عنوان اقدامات پیشگیرانه انجام پذیرد به شرح ذیل است.

- اطلاعات حساس و مهم نبایستی تنها در یکجا ذخیره گردند. به عبارت دیگر، بایستی از اطلاعات حساس حداقل یک نسخه پشتیبان تهیه گردیده و در فضای دیگری غیر از فضای ذخیره‌سازی[۵] اصلی نگهداری شود. بدین منظور توصیه می‌گردد فضای ذخیره‌سازی داده‌های پشتیبان تنها در زمان پشتیبان‌گیری و بازیابی داده‌ها به شبکه محلی متصل گردیده و در سایر مواقع اتصال آن به شبکه قطع گردد. در روال پشتیبان‌گیری از داده‌ها توجه گردد که عملیات مذکور به صورت منظم و در بازه‌های زمانی منطقی انجام پذیرفته و پس از انجام عملیات آزمون بازیابی و اطمینان از صحت آنها در محلی امن ذخیره گردد.
- تمامی سیستم‌عامل‌ها و نرم‌افزارهای موجود بایستی به صورت مداوم به‌روزرسانی گردیده و همواره آخرین وصله‌های امنیتی بر روی آن‌ها نصب شود.

[۵] Storage

- آنتی‌ویروس شبکه کاربران و سرورها می‌بایست به صورت مداوم به‌روزرسانی شده و تمام موارد سریعا به کامپیوترها و سرورهای شبکه اعمال گردد. از اینرو لازم است از آنتی‌ویروس‌های معتبر و تجاری که به‌روزرسانی خودکار دارند استفاده شود.
- بایستی از سیستم‌های ممانعت از نفوذ (IPS) و فایروال استفاده نموده و به صورت مداوم به‌روزرسانی گردد. همچنین باید فایروال سیستم‌عامل‌های تمامی کاربران و سرورها فعال شود.
- برای استفاده عادی و روزانه از سیستم نبایستی از کاربر با دسترسی Administrator یا root استفاده نمود. بایستی کاربری با سطح دسترسی محدود تعریف گردیده و از آن استفاده شود.
- ماکروها در مجموعه آفیس (Word، Excel، PowerPoint و غیره) غیرفعال گردد.
- افزونه‌های Adobe Flash، Adobe Reader، Java و Silverlight از مرورگر حذف گردند. در صورت لزوم به استفاده از این افزونه‌ها، با انتخاب تنظیمات مناسب، مرورگر به ازای هر بار نیاز به اجرای این افزونه‌ها، از کاربر تاییدیه درخواست نماید. همچنین لازم است افزونه‌های منسوخ شده[۶] نیز از مرورگر حذف گردیده و سایر افزونه‌ها همواره به‌روزرسانی شوند.
- سرویس‌ها و پروتکل‌های غیر مورد نیاز یا نا امن (آسیب‌پذیر) بر روی سرورها غیرفعال گردد. به عنوان نمونه، می‌بایست SMBv1 بر روی تمامی سیستم‌عامل‌های شبکه سرورها و کاربران غیرفعال شود.
- از مشاهده و مرور وب‌سایت‌های مشکوک پرهیز گردد.
- هرزنامه‌ها و ایمیل‌های از سوی فرستنده ناشناس باز نگردد. از دانلود فایل‌های پیوست ایمیل‌های مشکوک اجتناب نموده و بر روی لینک‌های مشکوک کلیک نشود.
- در سطح شبکه کاربران از ایمیل‌های غیرسازمانی استفاده نگردد.
- در صورتیکه سروری به/از اینترنت سرویس نمی‌دهد/نمی‌گیرد، بایستی دسترسی سرور مذکور به اینترنت قطع گردد.
- ارتباط تمامی فضاهای ذخیره‌سازی خارجی بایستی با سایر تجهیزات قطع بوده و فقط با استفاده از سرور واسط و مجهز به سرویس FTP ذخیره گردد.
- دسترسی DNS داخلی به اینترنت قطع گردد. همچنین بایستی سرور DNS شبکه داخلی و عمومی از یکدیگر تفکیک شوند.
- توصیه می‌شود سیستم‌های کاربران در زمان اتمام ساعت کاری حتما خاموش گردند.

۵-۲- اقدامات واکنشی

درصورت آلوده شدن به باج‌افزار بایستی توجه شود که در اغلب موارد امکان رمزگشایی فایل‌های رمز شده وجود ندارد. با این اوصاف، توصیه می‌شود در صورت مواجهه با باج‌افزار موارد ذیل رعایت گردد.

- به هیچ عنوان سیستم آلوده را خاموش یا راه‌اندازی مجدد ننموده و هیچ پروسسی از سیستم Kill نشود.
- به هیچ وجه فایل‌های رمز شده حذف نگردد. چرا که ممکن است در آینده روشی برای رمزگشایی این فایل‌ها (بدون پرداخت باج) فراهم گردد.

---

[۶] Outdated

- در صورت اتصال رسانه های ذخیره‌سازی پشتیبان (Backup Storage) به سیستم های آلوده، فوراً جدا شوند.
- در اغلب موارد پرداخت‌کنندگان باج نیز به دلایل مختلف قادر به رمزگشایی فایل‌های خود نبوده‌اند. از اینرو توصیه می‌شود از پرداخت باج خودداری گردد.
- در برخی موارد ممکن است در اثر ضعف باج‌افزار در امحا نمودن نسخه اصلی فایل‌ها، امکان بازیابی بعضی از فایل‌های حذف شده با استفاده از ابزارهای File Recovery میسر باشد.
- در موارد محدودی نیز ممکن است به دلیل ضعف باج‌افزار در پیاده‌سازی عملیات رمزنگاری، ابزارهایی برای رمزگشایی فایل‌های رمز شده توسط این باج‌افزار ارائه گردد.