آشنایی با باج افزارها و روش های آلودگی

اداره فناوری اطلاعات و ارتباطات

سال ۱۳۹۷

باج افزار(Ransomware) چیست؟

باج افزار نوع جدیدی از بدافزارها(Malware) است که پس آلوده کردن رایانه ای، ابتدا فایل ها را کد گذاری (Encrypt)می کند و سپس از کاربر رایانه می خواهد برای رمز گشایی(Decrypt) اطلاعات خود، مبلغی را بپردازد. این کار در حقیقت یک نوع اخاذی مدرن است. برخی از انواع آن ها روی فایل ها رمزگذاری انجام می دهند و برخی دیگر ممکن است رایانه را قفل کنند و پیام هایی روی نمایشگر نشان دهند که از کاربر می خواهد مبالغی را واریز کند. باج افزار به غیر از باج خواهی از قربانی، سعی می کند خود را در سایر دستگاه های متصل تکثیر نموده و حیطه کار خود را گسترش دهد.

انواع باج افزار

بدافزارها (Scareware)

به باج افزاری که تنها برای ایجاد نگرانی یا ترس درکاربر ناآگاه طراحی می شود ترس افزار(Scareware) می گویند.این باج افزار معمولاً با استفاده از یک سری ترفند، کار می کند که کاربر تصور کند دستگاهش به یک ویروس رایانه ای یا دیگر برنامه های مخرب آلوده شده است و تنها اجرای برنامه ترس افزار است که می تواند این تهدید را بر طرف کند. به محض اینکه کاربر این برنامه را دانلود و نصب کرد ممکن است برنامه مخرب دیگری نیز هم زمان بر روی رایانه وی نصب گردد که می تواند اطلاعات شخصی کاربر را سرقت نماید و یا از راه دور به دستگاه کاربر دسترسی داشته باشد و از این طریق حملات دیگری را اجرا کند؛ اما ممکن است هدف بدافزار تنها واریز پول به حساب تولیدکننده آن طریق خرید یک برنامه ضدویروس یا برنامه افزایش کارایی سیستم و یا دیگر برنامه های قانونی باشد. این دسته ساده ترین نوع باج افزار است.

Lock Screen Viruses یا مسدودکننده ها

این دسته که به Lock - Screen Viruses یا مسدودکننده ها معروف است صفحه نمایش را قفل کرده و به هیچ طریق اجازه استفاده از رایانه را نمی دهد. پس از شروع ویندوز یک پنجره به اندازه صفحه نمایشگر باز می شود و معمولاً می گوید که از طرف یکی از نهادهای اجرای قانون است و شما قانونی را نقص کردید و باید جریمه پرداخت کنید.

The Really Nasty Stuff

بدترین نوع باج افزارها می باشند؛ مانند Wanna Cry , Locky ، زیرا تا زمانی که شما مبلغی را پرداخت نکنید فایل ها را رمزگذاری شده نگه می دارد و یا حتی با پرداخت پول هم قابل بازگرداندن نیست. در این گونه موارد برای بازیابی اطلاعات می بایست قبلاً نسخه پشتیبان تهیه کرده باشید. بزرگ ترین تفاوت بین دو نوع باج افزار مسدود کننده و رمزگذار این است که صدمات مسدودکننده ها قابل برگشت است. حتی در بدترین حالت، صاحب رایانه آلوده می تواندسیستم عامل را دوباره نصب کند و همه فایل هایش را برگرداند. ولی باج افزارهای رمز گذار مطمئناً بسیار پیچیده تر هستند زیرا در حالت کلی امکان ندارد فایلی بدون کلید رمز گشایی، بازگردانیده شود. معمولاً این کلیدها روی سرورهای مجرمان ذخیره می شوند و قربانیان به آن دسترسی ندارند.

چطور ممکن است دستگاهی به باج افزار آلوده گردد؟

کاربر ندانسته یا ناخواسته فایل آلوده (Infected File) به باج افزار را دریافت می کند. بیشتر رایانه ها زمانی به باج افزارها آلوده می شوند که فرد از طریق یک ایمیل ساختگی (Phishing/Fishing) به استفاده از یک وب سایت آلوده به بدافزار، ترغیب می شود. در برخی از موارد نیز هنگامی که فرد روی فایل ضمیمه شده به ایمیل کلیک می کند، باج افزار به صورت پنهانی بر روی سیستم وی نصب می شود. در روشی دیگر باج افزارها در بستر شبکه اینترنت یا اینترانت، با استفاده از آسیب پذیری (Vulnerability) ناشی از حفره های امنیتی (Security Hole) یا نقض امنیتی (Security Bug or Security Defect) سیستم عامل یا سایر نرم افزارهای کاربردی به دستگاه شخص یا سازمان رخنه کرده ضمن تکثیر خود اقدام به رمزگذاری فایل ها و اخاذی می کنند.

نحوه ی کار باج افزار های رمز کننده در سیستم قربانی

- هنگامی که باج افزار روی سیستم قربانی وارد شود به یکی از دامنه های مشخص شده(سایت مرجع ویروس) وصل می شود و کلید عمومی رمزگذاری خود را دانلود می کند.
- بیشتر به دنبال فایل هایی با پسوندهای مشخص مانندpdf و docx می گردد.

برای هر فایل یک کلید تولید و آن را رمزنگاری می کند و کلید رمز شده را اول هر فایل می نویسد.

- پیغام باج خواهی برای قربانی نمایش داده می شود و نحوه پرداخت را از طریق بیت کوین به قربانی اعلام می کند.
- در برخی موارد مهاجم پس از پرداخت پول، کلید رمزگشایی را برای قربانی ارسال می کند.
- در تمامی مراحل ویروس سعی بر تکثیر خود به سایر دستگاه های متصل/ مرتبط می نماید.

مهم ترین و خطرناک ترین باج افزار های حال حاضر

***باج افزار کریپتولاکر CryptoLocker**

***باج افزار WannaCry**

***باج افزار پتیا Petya (برخی از صاحب نظران، نسخه جدید این وَرم را جزو دسته بندی باج افزارها محسوب نمی نمایند.)**

باج افزار واناکرای(Wannacry)

Wannacrypt که بهWannacryنیز شهرت یافته است، مانند دیگر باج افزارها(Ransomwares) فایل های رایانه ی قربانی را رمزگذاری می کند و فقط در ازای دریافت مبلغی به عنوان باج، کلید رمز را به کاربر می دهد. این باج افزار با استفاده از نقصی امنیتی در سرویس SMB (File Sharing ویندوز برای تکثیر خود بهره می گیرد. این روش که Eternal Blue نامیده می شود، در ماجرای نفوذ به NSA(سازمان امنیت آمریکا) در سال گذشته توسط هکرهایی که خود را Shadow Brokers می نامیدند، لو رفته است. ماکروسافت آپدیت MS۱۷-۰۱۰ را در ماه مارس ۲۰۱۷ برای رفع این نقص منتشر نمود؛اما بسیاری از کاربران و سازمان ها که رایانه های خود را تاکنون به روزرسانی نکرده اند، در مقابل این حمله ی سایبری کاملاً بی دفاع هستند. این کرم رایانه ای به گونه ای عمل می کند که تنها یک رایانه در شبکه آلوده شود، فوراً به دنبال دیگر رایانه های آسیب پذیر می گردد و آنها را نیز آلوده می کند. به گفته ی مایکروسافت عملکرد این کرم رایانه ای به گونه ای است که در شبکه به دنبال ویندوزهایی می گردد که آپدیت مایکروسافت را برای

رفع باگ Eternal Blue دریافت نکرده باشند و آن ها را آلوده می کند. در همین حال، با اسکن آدرس های مرتبط در اینترنت سعی می کند دستگاه های آسیب پذیر را بیابد و خود را تکثیر کند که این عمل منجر به ترافیک سنگینی در سرور از سوی هاست های آلوده می شود.

باج افزار پتیا(Petya)

Petya که در محافل امنیت سایبری با نام پتیا (Petya) نیز شناخته می شود، از اواخر ماه مارس سال ۲۰۱۶، فعالیت خود را آغاز کرده بود اما نسخه تغییر یافته آن از ژوئن ۲۰۱۷ شروع به انتشار کرد و موجب آلوده شدن بسیاری از سازمان ها و شرکت ها شد.جالب اینجاست که این باج افزار نیز همانند واناکرای از آسیب پذیری SMB (File Sharing) برای انجام حملات و گسترش خود استفاده می کند. باج افزار پتیا طوری طراحی شده تا آلودگی گسترده ای را ایجاد کند. این باج افزار برای ایجاد آلودگی از آسیب پذیری اترنال بلو(Eternal Blue) استفاده می کند و زمانی که از این آسیب پذیری با موفقیت استفاده شد، باج افزار خود را در سیستم هدف کپی کرده و اجرا می شود. سپس Petya شروع به رمزنگاری فایل ها وMBR هارد کرده و یک زمان بندی برای ریبوت کردن سیستم پس از یک ساعت به کار گرفته می شود. چیزی که پتیا را از دیگر باج افزارها متمایز می کند این است که به جای ویندوز از سیستم عامل کوچک خود استفاده می کند و به همین دلیل می تواند ساختار های حیاتی سیستم فایل کامپیوتر را در صورت راه اندازی مجدد آن روی دیسک بوت نیز رمزنگاری کند. در صورتی که فایل های سیتم توسط باج افزار پتیا رمزنگاری شود، دیگر هیچ روشی برای بازگرداندن آن وجود نخواهد داشت و در حال حاضر، پیش گیری تنها راه حل موجود برای مقابله با این باج افزار است؛ حتی در صورت پرداخت وجه درخواست نیز تضمینی برای رمزگشایی فایل ها وجود ندارد. اگر سیستم به شکل موفقیت آمیزی آلوده شود، پتیا صفحه ای را به زبان انگلیسی به نمایش در می آورد و از کاربر خواسته می شود تا ۳۰۰ دلار پول را در قالب بیت کوین به کیف پولی که به آدرس posteo.net متصل است واریز کند؛ اما نکته مهم این است که بعد از آلوده شدن سیستم به این ویروس کلیه اطلاعات ذخیره شده بر روی سیستم از بین می رود و امکان بازیابی آن ها حتی برای افرادی که رمزنگاری ویروس را نوشته اند نیز وجود ندارد.

روش های توصیه شده جلوگیری از آلوده شدن به باج افزارها در شهرداری تهران

- مطابق روال های تعیین شده امنیتی سازمان فناوری اطلاعات و ارتباطات اقدام نمایید.

- اطلاعات خود را به روز نمایید و از آخرین اطلاعیه های امنیتی و هشدارها آگاهی داشته باشید .

- آگاهی رسانی و آموزش به کلیه کاربران در خصوص رعایت الزامات امنیتی را انجام دهید.

- از نصب و به روز بودن آنتی ویروس سازمانی بر روی کلیه دستگاه های واحد تابعه اطمینان حاصل نمایید.

- کلیه نرم افزارهای غیرضروری را از روی سیستم ها حذف نمایید.

- از نصب و فعال بودن (Agent) دسکتاپ سنترال بر روی کلیه دستگاه های واحد تابعه خود اطمینان حاصل نمایید.

- وصله های امنیتی (ارائه شده در مسیر زیر) را به وسیله دسکتاپ سنترال بر روی همه دستگاه های واحد تابعه نصب نموده و از صحت نصب آن ها بر روی همه دستگاه ها اطمینان حاصل نمایید.

ftp://ftp.tehran.iri/Security/patch٪۲۰ Management

نصب وصله امنیتی MS۱۷-۰۱۰ (KB۴۰۱۲۲۱۲ برای سیستم عامل Windows۷ و KB۴۰۱۲۵۹۸ برای سیستم عامل Windows XP SP۳) به وسیله دسکتاپ سنترال بر روی کلیه دستگاه های واحد تابعه و اطمینان از صحت نصب آن بر روی کلیه دستگاه ها (دریافت از مسیر زیر)

ftp://ftp.tehran.iri/Security/patch٪۲۰ Management/Wanna ٪۲۰ Cry ٪۲۰ Patch

- عدم استفاده از پروتکل Share در کلیه واحدهای تابعه

عدم استفاده از فلش آلوده (قبل از استفاده از فلش آن را با آنتی ویروس به روز شده اسکن نمایید)

پایش و نظارت مستمر بر روی ترافیک شبکه و رخدادهای دستگاه های کاربران، تحلیل و ریشه یابی موارد مشکوک، اقدام جهت رفع و ارسال گزارش های تحلیلی و اقدامات صورت پذیرفته

- پشتیبان گیری از داده های حساس کاربران در رسانه ای مطمئن

-در صورت دریافت تهدیدهای امنیتی از سوی سایر واحدهای تابعه، جهت رفع مشکل صورت گرفته با راهبر شبکه و امنیت آن واحد هماهنگی لازم را انجام دهید و ضمن ثبت در سوابق خود، سازمان فناوری اطلاعات و ارتباطات را از وقوع آن تهدیدها مطلع نمایید.

-این باج افزار بر روی ویندوزهای ۸/۱ و ۱۰ نیز تاثیر مخربی می گذارد. لذا برای مصونیت از این باج افزار بر روی ویندوزهای ۱۰ و ۸/۱ روش زیر بکار گرفته شود.

Open Control Panel, clik programs, and then clik Turn Windows features on or off CIFS File Sharing Support checkbox, and then click Ok to close the window/In the Windows Features Window, clear the SMB ۱,۰ Restart the System.

****

روش های عمومی جلوگیری از آلوده شدن به باج افزارها

- به روز بودن و مسدود کردن حفره های امنیتی
- انتخاب رمزهای عبور مناسب و امن و تغییر آن در بازهای زمانی کوتاه
- نادیده گرفتن ایمیل های غیر ضروری
- قطع ارتباط با شبکه هنگام آلوده شدن
- به حداقل رساندن استفاده از Pluginهای مرورگر و استفاده از مسدودکننده ها برای محافظت در برابر تبلیغات مخرب
- بدون در نظر گرفتن ملاحظات امنیتی نرم افزارهای پیشنهادی وب سایت ها را نصب ننمایید.
- استفاده از آنتی ویروس مناسب برای محافظت از سیستم
- به روز نگهداری سیستم عامل و ت مام نرم افزارهای نصب شده
- پاک کردن کلیه نرم افزارهای غیر ضروری از روی سیستم
- اسکن ذخیره سازهای USB قبل از استفاده، توسط آنتی ویروس به روز شده
- ایجاد نسخه های پشتیبان از اطلاعات حساس کاربر (خارج از فضای هارد کاربر)