باج افزار چیست؟

باج‌افزارها گونه‌ای از بدافزارها هستند که دسترسی به سیستم را محدود می کنند و ایجادکننده آن برای برداشتن محدودیت درخواست باج می کند. برخی از انواع آنها روی فایل های هارددیسک رمزگذاری انجام می‌دهند و برخی دیگر ممکن است به سادگی سیستم را قفل کنند و پیام هایی روی نمایشگر نشان دهند که از کاربر می خواهد مبالغی را واریز کنند . باج‌افزارها ابتدا در روسیه مشاهده شدند اما اخیراً تعداد حملات باج افزارها به کشورهای دیگر از جمله استرالیا، آلمان و ایالات متحده آمریکا و حتی ایران افزایش یافته است.

عملکرد باج افزارها

عملکرد باج افزارها به این صورت است که ابتدا فایل های سیستم یک شخص، یک سازمان و یا یک مرکز تجاری را کدگذاری می کند و سپس از کاربران سیستم ها می‌خواهد برای رمزگشایی مجدد اطلاعات خود مبلغی را بپردازند. این کار در حقیقت یک نوع اخاذی مدرن است.

باج افزارها از طرق مختلف مانند کرمها منتشر می شوند و پس از نصب و اجرا شروع به اعمالی مانند رمزگذاری هارددیسک می کنند. باج افزارهای پیشرفته تر با استفاده از کلید عمومی فایلها را رمز نگاری می کنند و کلید خصوصی لازم برای بیرون آوردن فایلها از حالت رمز شده تنها در دستان طراح باج افزار است و کاربر برای بازکردن فایلهایش مجبور به پرداخت وجه به حساب طراح باج افزار می شود. برخی دیگر از باج افزارها رمزگذاری انجام نمی دهند، بلکه از روش های دیگری مثل اختصاص پوسته سیستم عامل به خود یا تغییر رکوردهای مربوط به بوت، استفاده از سیستم را مختل می کنند.

باج افزارها برای دریافت پول از کاربر پیامهای مختلفی به او نمایش می‌دهند

این مبلغ اغلب به روشی از کاربر گرفته می شود که قابل باز پس گیری نباشد . مثلاً از طریق پیام کوتاه شارژی یا سیستم Ukash(پرداخت آنلاین).به تازگی استفاده از پول الکترونیکی بیت کوین مرسوم تر شده است .باج افزارها روشی برای کسب درآمد غیرقانونی هستند. هکرها می‌توانند از طریق باج افزارها درآمدی بین چند صد دلار تا چند هزار دلار کسب کنند. معمولا درخواست هکرها این است که وجه مورد نظر با استفاده از پول دیجیتالی بیت کوین پرداخت شود؛ زیرا ردیابی فردی که پول از این طریق به او پرداخته می شود؛ غیر ممکن است و هر چقدر در پرداخت وجه درخواست شده تعلل شود، نفوذ باج افزار به سیستم بیشتر می شود.

سیستم چگونه آلوده به باج افزار می شود؟

باج افزارها چه بخواهند سیستم های مراکز بزرگ و مهم مانند یک بیمارستان یا یک سازمان را آلوده کنند و چه بخواهند کامپیوتر شخصی یک فرد معمولی را مورد هدف قرار دهند، به یک شیوه عمل می کنند . بیشتر کامپیوترها زمانی به باج افزارها آلوده می شوند که فرد از طریق یک ایمیل فیشینگ ساختگی (ایمیلی که برای فریب افراد جهت به دست آوردن اطلاعات شخصی همانند رمز عبور، اطلاعات بانکی و ... مورد استفاده قرار می گیرد) برای استفاده از یک وب سایت آلوده به بدافزار، ترغیب می شود. در برخی از موارد نیز هنگامی که فردی روی فایل ضمیمه شده به ایمیل کلیک می کند، باج افزار به صورت پنهانی بر روی سیستم نصب می شود.برخی از مواردی که باعث آلوده شدن سیستم به باج افزار می‌شود، عبارتند از:

۱. باز کردن یک ایمیل حاوی ضمیمه مخرب
۲. کلیک روی لینک های مخرب که در ایمیل، شبکه های اجتماعی یا سایت ها قرار دارد.
۳. بازدید از سایت های مخرب که اغلب دارای ماهیت مستهجن هستند.
۴. باز کردن فایل های آلوده از فایل دیجیتال شرکت های حمل و نقل مبتنی بر وب
۵. باز کردن ماکروهای فاسد در اسناد برنامه (مثل واژه پرداز ها و صفحه گسترها)
۶. اتصال به دستگاه های جانبی USB مثل memory ، هارد اکسترنال ، mp3 playerو...
۷. استفاده ازCDیا Floppy های فاسد در کامپیوتر خود

هرزنامه (Spam)

یکی دیگر از راه های نفوذ باج افزارها، هرزنامه ها هستند که معمولا دارای فایل پیوستی از نوع (word,pdf,excel,) می‌باشند که با کلیک بر روی فایل ظرف مدت چند دقیقه کلیه اطلاعات کامپیوتر رمز می شود. با توجه به فرمول زیر میتوان راه نفوذ باج افزار از طریق Spam را نتیجه گرفت.

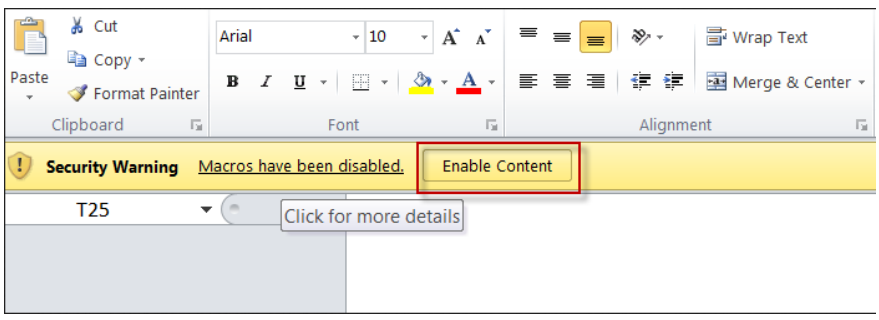
Unknown Email + Attachment (word, excel, zip, pdf)+ invoice = Ransomware

Spam از کجا می‌آید؟

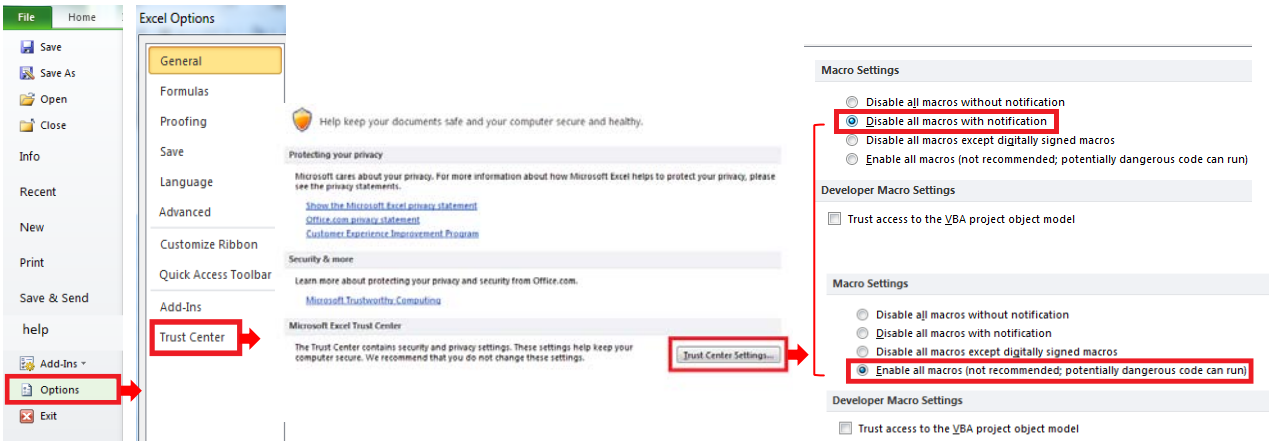
معمولا هرزنامه ها با عضویت در سایت های مختلف بوجود می آیند. به این صورت که با عضو شدن در سایتهای مختلف ایمیل هایی با توجه به علاقه مندی کاربر به صورت هرزنامه برای وی ارسال می شود که همین ایمیل میتواند حاوی باج افزار و ویروس باشد. بنابراین توصیه می شود ایمیل کاری را از ایمیل های دیگر مجزا کنیم تا در این زمینه دچار مشکل نشویم.

ماکروها

از دیگر راه های نفوذ باج افزار ها ماکروهای Office می‌باشد که رایج ترین ماکرو تبدیل تاریخ شمسی به میلادی و برعکس آن می باشد. باج افزار به این ماکرو تزریق و به کامپیوتر نفوذ می‌کند. معمولا به هنگام کار با Office پیغامی بر روی صفحه ظاهر می‌شود و درخواست فعال کردن ماکرو می دهد، که فعال کردن ماکرو راهی برای نفوذ باج افزار فراهم می کند.



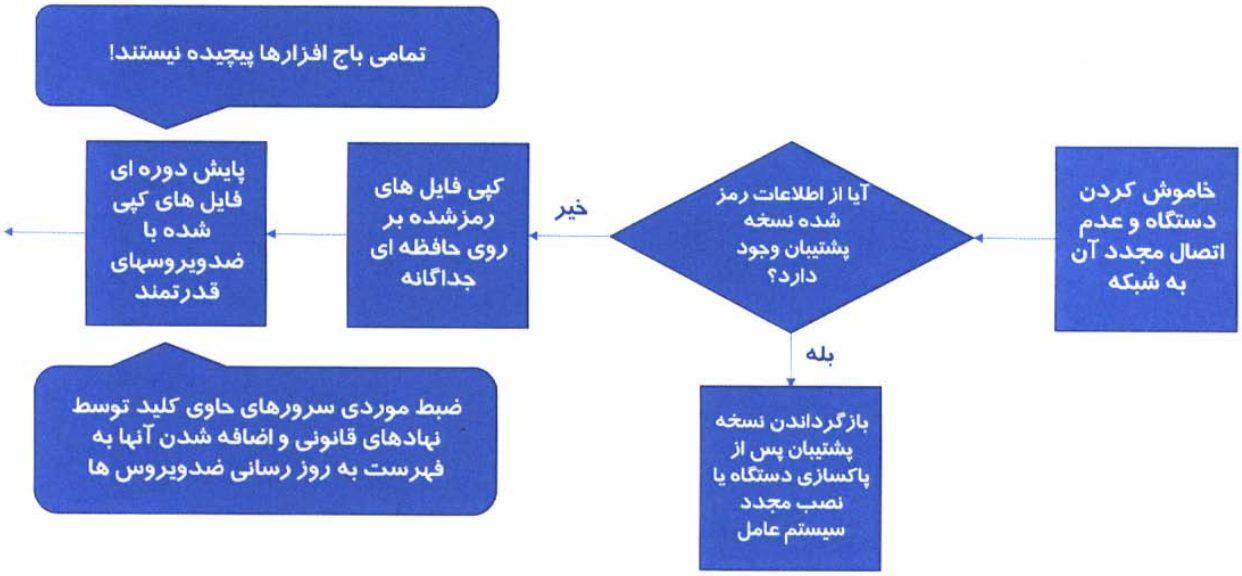
برای جلوگیری از این اتفاق میتوان ماکروها را غیرفعال کرد و فقط ماکرو مورد نیاز را فعال نمود:



موارد دیگر

- ✓ از دیگر عواملی که باعث حمله باج افزارها به کامپیوتر می شود، به روز نبودن نرم افزارهای مورد استفاده می باشد. به این منظور لازم است نرم افزارها را Update نموده و تا حد امکان از نسخه های جدید نرم افزارها استفاده نمود .(به عنوان مثال به روز بودن Browser ها یکی از این موارد می‌باشد.)
- ✓ مورد دیگری که می توان به آن اشاره نمود هنگام استفاده از سایتهایی همانند youtube,Aparat,... است که درخواست update یا نصب برنامه Adobe flash player می‌کند و لینکی را نیز در این مورد پیشنهاد می کند. در این مواقع از کلیک بر روی لینک خودداری نموده و برنامه را از سایت معتبر به صورت جداگانه دانلود و سپس نصب نمایید.
- ✓ بسیار اتفاق افتاده است که به هنگام نصب یا دانلود برنامه، موزیک و ... پی در پی لینکهایی مشاهده میشود که با کلیک بر روی آن امکان نصب یا دانلود فراهم می شود. در واقع از طریق این لینکها کاربر به سایتهای دیگری ارجاع داده می‌شود. این روش هم میتواند راهی برای نفوذ باج افزارها باشد، بنابراین لازم است از کلیک بر روی لینکها و هدایت به سوی سایتهای دیگر خودداری شود .(به طور مثال به هنگام دانلود فایل MP3 و درخواست نصب برنامه inlivid و هدایت کاربر به سایتها و لینکهای دیگر برای نصب برنامه)
- ✓ سایتهای تبلیغاتی نیز از موارد دیگر می باشد. به طور مثال به هنگام باز نمودن یک سایت مشاهده می شود سایتهای دیگری نیز به طور همزمان باز می‌شوند.
- ✓ نصب add-on های Browser ها بدون آگاهی از کاربرد آن و همچنین Update بودن آنها نیز میتواند راهی برای نفوذ باج افزارها باشد.

راهکار در زمان آلودگی



چگونه از سیستم خود در برابر باج افزارها محافظت کنیم؟

نحوه محافظت از سیستم در برابر باج افزارها همانند محافظت از آن ها در برابر یک بدافزار است . احتیاط، کلید اصلی جلوگیری از آلوده شدن یک سیستم به باج افزارها است . اگر چه این کار همیشه آسان نیست؛ اما در ادامه راهکارهایی را ارائه می دهیم که می تواند به ما در رابطه با این موضوع کمک کند .

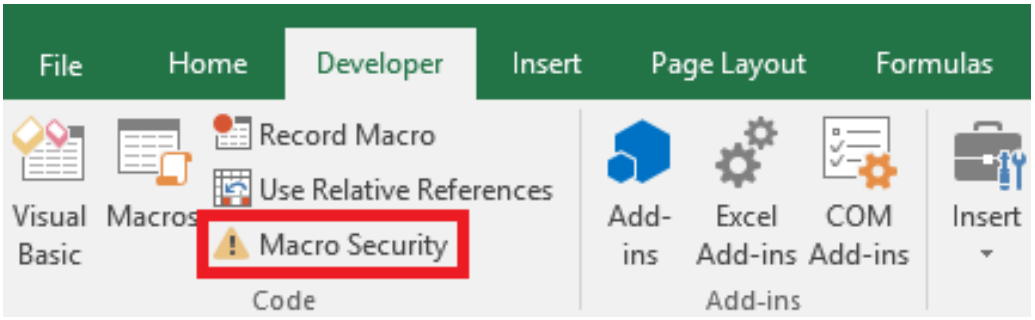
۱. بهتر است که روی لینک های موجود در ایمیل ها کلیک نکنی م و خود مان آدرس مورد نظر را در نوار آدرس مرورگر وارد کنیم.
۲. هرگز فایل های ضمیمه شده به ایمیل را بدون اطلاع از محتوای آن ها باز نکنی م و تنها در صورتی این کار را انجام دهیم که منتظر دریافت چنین فایل هایی هستیم و از محتوای آن ها نیز کاملا مطلع هستیم .
۳. هیچ گاه به ایمیل های ناشناس پاسخ ندهیم یا ایمیل هایی را که در قسمت spam ایمیل قرار دارد را باز نکنیم .
۴. هرگز نرم افزاری را تنها به خاطر درخواست یک وب سایت نصب نکنیم .
۵. همیشه یک فایل پشتیبان از اطلاعات شخصی کامپیوتر خود تهیه کنیم و آن را در یک درایو مجزا که دسترسی به آن از طریق سیستم ابری ممکن باشد، ذخیره کنیم . در این صورت در بدترین حالت هم می توانیم به مهمترین اطلاعات خود دسترسی داشته باشیم . البته باید به این نکته توجه داشته باشیم که برخی از باج افزار ها می توانند حتی فایل های مبتنی بر ابر ذخیره سازی را نیز آلوده کنند، بنابراین لازم است به طور منظم از اطلاعات خود نسخه پشتیبان تهیه کنیم .
۶. تنها از وب سایت های امن یا وب سایت هایی که می شناسیم استفاده کنیم .
۷. قبل از آنلاین شدن، از وجود آنتی ویروس و دیوار آتش مؤثر و به روز روی کامپیوتر خود مطمئن شویم و در صورتی امکان از antispyware نیز استفاده کنیم .

راه‌های پیشگیری و مقابله

✓ لازم است به هنگام دریافت ایمیل به خطوط قرمز رنگ توجه بیشتری نمود.

✓ در زمان باز نمودن سایت به آدرس آن نیز دقت کنیم و فقط به ظاهر سایت اکتفا نکنیم.

- ✓ غیرفعال کردن ماکروها



- ✓ استفاده از ضد ویروس قدرتمند و به روز رسانی مداوم آن
- ✓ بکارگیری نرم افزارهای پیشگیری از نفوذ
- ✓ نصب آخرین اصلاحیه های امنیتی
- ✓ تهیه پشتیبان از داده های با اهمیت بصورت دوره‌ای
- ✓ بهره گیری از نرم افزارها و سخت افزارهای ضد هرزنامه
- ✓ مسدود کردن ایمیل های با پیوست حاوی ماکرو در درگاه شبکه
- ✓ محدود کردن سطح دسترسی کاربران
- ✓ استفاده از دیواره آتش در درگاه شبکه
- ✓ بکارگیری بخش Access Protection در نرم افزار McAfee در مواقع لزوم