باج افزار یا **Ransomware** گونه ای بدافزار است که دسترسی به فایلهای کاربر را محدود ساخته وبرای دسترسی مجدد ، از او درخواست باج می کند. در سالهای اخیر آن دسته از باج افزار هایی که از طریق رمز نگاری اقدام به محدود سازی دسترسی کاربر به فایلها می کنند ، موفقیت های بی مثالی را نصیب صاحبان تبهکار خود کرده اند و بر اساس آمار، تعداد این باج افزارها به شدت در حال افزایش است.

در این نوع محدود سازی، هدف از رمز کردن، تغییر ساختار فایل است. به نحوی که تنها با در دست داشتن کلید رمز گشایی بتوان به محتوای فایل دسترسی پیدا کرد.

پیچیدگی و قدرت این کلیدها بر اساس تعداد بیت بکار رفته در ساختار کلید است. هر چه تعداداین بیت ها بیشتر باشد ، شانس یافتن آن هم دشوارتر و در بیت بالا عملا غیر ممکن می شود.

تاریخچه باج افزارها

❖ سال ۱۳۶۸

نخستین باج افزاری که کامپیوترها رو از طریق دیسک فلاپی آلوده می کرد شناسایی شد

باج افزار Reveton که با یک اسب تروای بانکی ترکیب شده بود با قفل کردن دستگاه از طریق نمایش یک تصویر ثابت اینطور القا می کرد که مسدود شدن دسترسی به دستگاه توسط نهادهای امنیتی و به دلیل نقص قوانین توسط کاربر صورت گرفته و کاربر می بایست برای دسترسی مجدد به دستگاه اقدام به پرداخت جریمه یا همان "باج" کند.

❖ سال ۱۳۹۴

باج افزار به عنوان سرویس "ransomware-os-o-software" وارد بازار تبهکاران سایبری شد. سرویس که تبهکاران بدون داشتن برنامه نویسی را نیز قادر به استفاده از این نوع بدافزارهای مخرب می کند.

سال ۱۳۹۵

تخمین زده می شود که سازنده Cerber سالانه نزدیک به یک میلیون دلار از راه عرضه خدمت :"باج افزار بعنوان سرویس" درآمد داشته باشد.

اصلی ترین اهداف نسل جدید باج افزارها

- ✓ شرکتهای کوچک و متوسط
- ✓ سازمانهای دولتی
- ✓ مراکز آموزشی
- ✓ مراکز درمانی
- ✓ موسسات مالی وبانکی
  - نیمی از شرکتها آلوده شدن به باج افزار را تجربه کرده اند.
  - برخی سازمانها هر هفته چندین بار به انواع باج افزارها آلوده می شوند.
  - در هر دقیقه بیش از ۱۰ باج افزار منحصر بفرد جدید شناسایی می شود.

دو دلیل برای افزایش باج افزارها

۱- حملات باج افزارها هم اکنون از حملات نشت اطلاعات پیشی گرفته است. دلیل آن اجرای ساده و سودده بودن این حملات برای صاحبان آنهاست.

۲- عدم امکان شناسایی باج گیران از طریق ردیابی مبالغ پرداختی، با توجه به استفاده آنها از پول های مجازی مانند بیت کوین.

آینده باج افزارها

- ✓ هدفمند تر شدن حملات باج افزارها
- ✓ اضافه شدن قابلیتهای پیشرفته فرار از سد امنیتی محصولات ودر نتیجه دشوارتر شدن شناسایی آنها
- ✓ هدف قرار گرفتن دستگاههای همراه و اینترنت اشیا بیش از قبل

راههای پیشگیری و مقابله با باج افزارها :

۱- آگاهی رسانی امنیتی بطور مستمر

آموزش صحیح کاربران می تواند صدمات ناشی از ایمیلهای وسوسه کننده مخرب را به طور چشمگیری کاهش دهد. کاربرانی که بیش از یک بار در طول سال آموزش می بینند با احتمال کمتری در دام ترفندهای مهندسی اجتماعی تبهکاران سایبری می افتند.

۲- شناسایی آسیب پذیری ها و اقدامات پیشگیرانه

- آسیب پذیری ها و نقاط ضعف امنیتی موجود بر روی سیستمها و شبکه سازمان را بیش از آنکه مورد بهره جویی مهاجمان قرار بگیرد شناسایی و ترمیم کنید.
- **نصب اصلاحیه ها وکنترل سطوح دسترسی**
  - سیستم های عامل و نرم افزارهای آنها را بروز نگه داشته و طح دسترسی کاربران به سیستم عامل و پوشه های اشتراکی را در کمترین حد ممکن قرار دهید.
- **استفاده از راهکارهای حفاظتی**
  - با استفاه از راهکارهای ضد ویروس، ضد هرز نامه، دیواره آتش، نفوذ یاب و کنترل برنامه ، بدافزارها و حملات را بصورت بلادرنگ شناسایی و مسدود کنید.
- **تهیه نسخه ی پشتیبان از سیستمها**
  - از داده های با اهمیت بصورت دوره ای و بنحو صحیح پشتیبان تهیه کنید. لازم به یادآوری است که برای تهیه نسخه پشتیبان به هارد اکسترنال اکتفا نکنید و اطلاعات مهم را روی DVD یا Blue ray نیز ذخیره نمایید.

- **به یاد داشته باشید که به ایمیلهای ناشناس و دعوت به کلیک کردن روی یک لینک یا باز کردن فایل پیوست از اشخاص ناشناخته توجه ننمایید.**

۳- برون خط شوید

در صورت آلوده شدن دستگاه به باج افزار، دشتکاه را خاموش کرده و اطمینان یابید دستکاه به شبکه داخلی سازمان و یا اینترنت دسترسی نداشته باشد.با توجه به زمان بر بودن فرآیند و رمز نگاری فایلها، البته در اکثر مواقع، خاموش کردن دستگاه ممکن است به نجات برخی فایلها کمک کند.

۴- بازگردانی اطلاعات

در صورت وجود نسخه پشتیبان از داده های رمز شده، دستگاه با دیسک نجات مجهز به آنتی ویروس راه اندازی شده و پس از انجام پویش و اطمینان از پاکسازی باج افزار ، داده ها برگردانده شود.

۵- پویش و حفظ داده های رمز شده

در صورت عدم وجود نسخه پشتیبان، دستگاه به همان روش مذکور پاک سازی شود. در نظر داشته باشید تمام باج افزار ها پیچیده نیستند و برخی از آنها تنها باج افزارهای رمز نگار نما هستند! بنابراین با پویش شدن ممکن است اطلاعات در ظاهر رمز شده به حالت قبل بازگردانده شود. پس از اطمینان از پاک سازی دستگاه ، فایلهای رمز شده بر روی حافظه ای نگه داری شود.

۶- از پرداخت باج پرهیز کنید.

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

۷- ردیابی نحوه آلوده شدن دستگاه

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

جدول ۱ : تاریخچه سند

نسخه	ویرایش	تاریخ	توضیحات
1.0	بهاره خشایی	۹۵/۱۱/۹	