



باج افزارها

باج افزار یک نوع نرم افزار مخرب (بدافزار) است که تمام داده ها را روی رایانه یا دستگاه تلفن همراه رمزگذاری کرده و دسترسی مالک آن ها را به این داده ها مسدود می کند. هنگامی که این آلودگی اتفاق می افتد، قربانی پیامی دریافت می کند که در آن دستورالعمل های چگونگی پرداخت باج (معمولاً در بیت کوین ها) ارائه شده است. فرآیند اخاذی اغلب شامل محدودیت زمانی برای پرداخت می شود. پرداخت جریمه باید کلید رمزگشایی را به قربانی بدهد، اما هیچ تضمینی وجود ندارد که این اتفاق بیفتد.

#باج افزار: یک نوع نرم افزار مخرب (بدافزار) است که تمام داده ها را روی رایانه یا دستگاه تلفن همراه رمزگذاری کرده و دسترسی مالک آن ها را به این داده ها مسدود می کند. هنگامی که این آلودگی اتفاق می افتد، قربانی پیامی دریافت می کند که در آن دستورالعمل های چگونگی پرداخت باج (معمولاً در بیت کوین ها) ارائه شده است. فرآیند اخاذی اغلب شامل محدودیت زمانی برای پرداخت می شود. پرداخت جریمه باید کلید رمزگشایی را به قربانی بدهد، اما هیچ تضمینی وجود ندارد که این اتفاق بیفتد.

1-1 دو نوع باج افزار رایج وجود دارد

1. باج افزار رمزگذاری، که شامل الگوریتم های رمزنگاری پیشرفته است. این برنامه برای مسدود کردن فایل های سیستم و تقاضای باج است و برای دسترسی قربانی به آن ها، کلیدی وجود دارد که می تواند محتوای مسدود شده را رمزگشایی کند. مثلاً CryptoLocker، Locky، CryptoWall.
 2. باج افزار مسدودکننده، که قربانی را به وسیله سیستم عامل مسدود می کند و امکان دسترسی به دسک و not تاپ و هر برنامه یا فایلی را غیرممکن می سازد. پرونده ها در این مورد رمزگذاری نمی شوند، اما مهاجمان باز هم برای کامپیوتر آلوده باج گیری می کنند. مثلاً باج افزار police-theme یا Winlocker.
- برخی از نسخه های مسدودکننده می توانند حتی MBR (Master Boot Record) را آلوده کنند. MBR بخشی از هارد دیسک کامپیوتر است که باعث می شود سیستم عامل بوت شود. هنگامی که باج افزار MBR رخ بدهد، فرآیند بوت نمی تواند به طور معمول انجام شود و باعث می شود اعلانی بر روی صفحه، نمایش داده شود. مثلاً خانواده های Satana و Petya.

باج افزار دارای برخی ویژگی های کلیدی است که آن را از دیگر نرم افزارهای مخرب مجزا می کند.

&bull؛ از ویژگی های آن رمزگذاری غیرقابل شکستن است، این بدان معنی است که شما نمی توانید فایل ها را خودتان رمزگشایی کنید (ابزارهای رمزگشایی مختلف وجود دارد که توسط محققان امنیت سایبری منتشر شده اند).