مهندسین مشاور سازه پردازی ایران (سهامی خاص)

SAZEH PARDAZI IRAN
Consulting Eng. Co

باج افزار ها

باج افزار چیست و چگونه عمل می کند؟

باج افزار گونه ای از بدافزارها است که گام های سریعتری را برداشته است و در حال حاضر به طور عجیبی در حال همه گیر شدن است.

- **باج افزارها دو نوع هستند:**
- **قفل کننده (کریپتورها) و مسدود کننده.**
- پس از آلوده سازی کامپیوتر، قفل کننده ها داده های ارزشمند شما از جمله اسناد، عکس ها، دیتابیس و غیره را رمزنگاری می کنند. هنگامی که آن ها در حال رمزنگاری هستند، هیچ فایلی باز نخواهد شد و کاربر قادر به دستیابی به هیچ کدام از آن ها نخواهد بود. مجرمان پشت این حمله موقعیتی عالی یافته اند، آن ها به ازای قرار دادن کلید رمزگشا برای بازگرداندن فایل های قفل شده درخواست باج می کنند .اما مسدود کننده ها همانطور که از اسم آن ها مشخص است وظیفه ی مسدود کردن را دارند، آن ها دسترسی به سیستم آلوده را مسدود می کنند، به این معنی که آن ها نه تنها دسترسی به فایل ها بلکه دسترسی به کل سیستم را مسدود می کنند. تقاضای باج مسدود کننده ها معمولا به اندازه ی قفل کننده ها نیست. هکرها می توانند 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 شما 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.

راه‌های بازیابی فایل‌های آلوده به ویروس باج‌گیر چیست؟

- متخصصان امنیت توصیه می کنند که هیچ وجهی به باج افزارها پرداخت نکنید در حالی که این کار یکی از راه های به دست آوردن کنترل کامپیوتر و باز پس گیری فایل ها و داده های آن است. بهتر است قبل از آلوده شدن، از اطلاعات خود یک نسخه پشتیبان تهیه کنید تا در صورتی که مقصد یک حمله قرارگرفتید، با آرامش و خونسردی هرچیزی را که لازم دارید از نسخه های پشتیبان خود بازگردانی نمایید. علاوه بر این، حتی اگر بسیاری از باج افزارها کنترل سیستم را بازگردانند، ممکن است همیشه مجددا در معرض آسیب باشید.
- حتی ممکن است مبالغ را پرداخت نموده اما همچنان کنترلی روی اطلاعات خود نداشته باشید. اگر فایل های شما ربوده شد و پشتیبان نیز نداشتید، بزرگترین اشتباه این است که انتظار داشته باشید راه حل حذف ویروس باجگیر به صورت آنلاین یافت شود و رمزگشایی فایل های آلوده توسط باج افزار بصورت آنلاین انجام گیرد.
- ابزارهای آنلاین اغلب برای نسخه‌های قدیمی باج افزارها در دسترس هستند در حالی که مهاجمین نرم‌افزارها و باج افزارهای خود را بصورت مداوم بروزرسانی نموده و روش‌های رمزنگاری خود را تغییر میدهند تا امکان بازگشایی رمزها وجود نداشته باشد. البته این موضوع به این معنی نیست که دست از کار کشیده و سیستم خود را رها نمایید.
- در این مواقع ما توصیه اکید میکنیم که در انجمن‌های فعال در حوزه امنیت عضو شوید در این انجمن ها از برخی از باج افزار ها مانند Locky, TeslaCrypt, CryptoWall, Petya, CryptXXX, Locker اطلاعات خوبی وجود دارد و امکان کمک به شما نیز بیشتر از راه های دیگر است. همچنین گزارش دادن این موضوع به پلیس فتا کمک خواهد نمود تا اگر یک جرم سازمان یافته در حال وقوع باشد، پلیس آنرا کشف نموده و از خطرات بیشتر پیشگیری شود.

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 به شما ارائه می دهیم که می تواند به شما در رابطه با این موضوع کمک کند.
- بهتر است که روی لینک های موجود در ایمیل ها کلیک نکنید و خودتان آدرس مورد نظر را در نوار آدرس مرورگر وارد کنید
- هرگز فایل های ضمیمه شده به ایمیل را بدون اطلاع از محتوای آن ها باز نکنید و تنها در صورتی این کار را انجام دهید که منتظر دریافت چنین فایل هایی هستید و از محتوای آن ها نیز کاملا مطلع هستید.
- هرگز وارد هر سایتی نشوید؛ مخصوصا سایت هایی که دارای محتوای مستهجن و فیلم های غیر اخلاقی هستند. کامپیوتر شما به راحتی می تواند با یک بار بازدید شما از سایت های غیر قابل اعتماد، آلوده به باج افزار شود.
- هرگز نرم افزاری را تنها به خاطر درخواست یک وب سایت نصب نکنید.
- همیشه یک فایل پشتیبان از اطلاعات شخصی کامپیوتر خود تهیه کنید و آن را در یک درایو مجزا که دسترسی به آن از طریق سیستم ابری ممکن باشد، ذخیره کنید. در این صورت در بدترین حالت هم می توانید به مهمترین اطلاعات خود دسترسی داشته باشید.

راه های مقابله با حملات باج افزارها

بهترین محافظت جلوگیری است.قدم های زیر را دنبال کنید تا از حملات باج افزار در امان بمانید.

۱ **سیستم خود را بروز رسانی کنیم**

مرورگرها؛سیستم عامل و سایرنرم افزارها را بروزرسانی کنید.

۲ **کاربران را آموزش دهید**

یکی از رایج ترین راه ها برای آلوده کردن دستگاه ها به باج افزار؛مهندسی اجتماعی است.یادبگیرید تا چگونه حملات فیشینگ؛وب سایت آلوده و اسپم را تشخیص دهید.

۳ **از فایل ها بک آپ بگیرید**

به طور منظم و امن و همچنین در چند نسخه چه آنلاین چه آفلاین از داده های خود بک آپ بگیرید.

مراقب باشید که فایل بک آپ را روی سیستم ذخیره نکنید. برخی از باج افزارها می توانند داده های پوشه مپ را نیز رمزگذاری کنند.

اگر روی حافظه داخلی یا خارجی دیگر بک آپ تهیه کردید ،مطمئن شوید که بعد از آن حافظه به دستگاه وصل نباشد.

پیشنهاد میکنم از فضاهای ابری که داده ها را رمزگذاری شده نگاه می دارند و از احراز هویت چند مرحله ای استفاده می کند برای بک آپ استفاده کنید.

۴ **امنیت چند لایه**

استفاده از چندین روش امنیت سایبری در شناسایی حمله بدافزار و جلوگیری از آلوده شدن دستگاه به آن کمک زیادی می کنند:

- ضد باج افزار
- ضد بد افزار
- آنتی ویروس
- ضد اکسپلویت
- دیوار آتش

اگر کامپیوتر شما به بدافزار آلوده شد؟

اگر فایل پشتیبان دارید،که بهتر است داشته باشید.این فایل را در کامپیوتر دیگری که آلوده نیست اسکن کنید تا مطمئن شوید به بدافزار آلوده نیست.پس دستگاه خودتان را پاکسازی کنید و فایل پشتیبانی را بازیابی کنید.