باج افزار

باج افزار یک نوعی از بد افزارها است که به مجرمان این امکان را می دهد تا بتوانند از طریق یک کنترل از راه دور، کامپیوتر قربانی را قفل کنند به طوری که کاربر نتواند از سیستم خود استفاده کند و سپس یک پنجره پاپ آپ روی کامپیوتر شخص نمایان کنند تا به او بگویند که این قفل باز نمی شود تا زمانی که هزینه ای را برای باز کردن آن بپردازید

گاهی اوقات مجرمان تنها قسمتی از کامپیوتر قربانی را که قابل دسترسی است، قسمت keypad یا صفحه کلید مجازی قرار میدهند که قربانی بتواند رمز را وارد و پول را پرداخت کند. جدید ترین نوع باج افزار که اخیراً شناسایی شده است، crypto locker است .گاهی هکرها با قرار دادن یک تصویر نامناسب روی کامپیوتر شخص یا اتهام فعالیت غیر قانونی به آن ها، شخص را تحت فشار می گذارند که هر چه سریع تر پول درخواستی آنها را پرداخت کنند تا هکر ها قفل کامپیوتر آنها را باز کنند

تاثیرات و مکانیسم باج افزار:

ممکن است کاربران با ابزارهای متفاوتی با تهدید این بد افزار مواجه شوند . باج افزارها میتوانند هنگامیکه کاربران به طور ناخواسته از وب سایت مخربی دیدن میکنند و یا هنگامیکه که یک برنامهی آلوده را دانلود میکنند، ممکن است بروی سیستم آنها بارگیری شود .راههای متفاوتی برای دسترسی باج افزارها به سیستم وجود دارد که برخی از آنها توسط ضمیمهی ویروسی که در ایمیلهای اسپم یا فیشینگ(هرزنامه ها)وجود دارد، در این حالت به محض کلیک کردن بروی لینک دریافتی، سیستمهای آسیب پذیر آلوده باج افزار میشوند. هنگامیکه بد افزار بروی سیستمهای آسیب پذیر اجرا میشود، میتواند صفحه کلید رایانه را قفل کند و به رمز نگاری فایلهای از پیش تعیین شده بپردازد .در نخستین گام، تصویری تمام صفحه روی سیستم آلوده نمایش داده میشود، که در اعلانی نامحسوس به قربانیان میفهماند که سیستم قفل شده است و تا هنگامیکه پرداخت باج را انجام ندهند قربانیان نمیتوانند به سیستم خود دسترسی داشته باشند. این مکانیسم و نحوه عملکرد، نشان دهنده پرداخت باج توسط کاربران را نشان میدهد. گام دوم، باج افزار به محض در برگرفتن سیستم، مانع دسترسی کاربران به فایلهای مهم و حیاتی، هم چون : اسناد و مدارک، و برنامه های گسترده (وب) میشود.

خطرات

زمانی که شما سهواً خطاهای زیر را انجام دهید، امکان دارد کامپیوتر شما درگیر باج افزار شود :

۱. باز کردن یک ایمیل حاوی ضمیمه مخرب.
۲. باز کردن پیوست ایمیلهای اسپم یا لینکهای درون آنها
۳. کلیک روی لینک های مخرب که در ایمیل، شبکه های اجتماعی یا سایت ها قرار دارد .
۴. بازدید از سایت های مخرب که اغلب دارای ماهیت مستهجن هستند.
۵. باز کردن فایلهای دانلود شده آلوده از سایتهای نامعتبر یا کلیک روی لینکهای مخرب
۶. باز کردن فایل های آلوده از فایل دیجیتال شرکت های حمل و نقل مبتنی بر وب.
۷. استفاده از روش های مهندسی اجتماعی برای هدایت کاربران به صفحات فیشینگ
۸. آلودگی از طریق سایتهای هک شده و یا شبکههای توزیع تبلیغات آلوده
۹. آلودگی از طریق هک و نفوذ به سیستمها؛ به خصوص سیستم هایی که پچ های رفع آسیب پذیری آنها به روز نشده است.
۱۰. باز کردن ماکرو های فاسد در اسناد برنامه (مثل واژه پرداز ها و صفحه گستر ها)
۱۱. اتصال به دستگاه های جانبی USB مثل memory ، هارد اکسترنال ، mp3 pl ayer و **تلفن همراه**
۱۲.استفاده از سی دی یا فلاپی های فاسد در کامپیوتر خود.

از کاربران خواهش می شود :

۱. هیچ گاه به ایمیل های ناشناس پاسخ ندهید یا ایمیل هایی را که در قسمت spam ایمیلتان قرار دارد را باز نکنید.
۲. تنها از وب سایت های امن یا وب سایت هایی که می شناسید استفاده کنید .
۳. قبل از آنلاین شدن، از وجود آنتی ویروس مؤثر و به روز روی کامپیوتر خود مطمئن شوید .
۴. به طور منظم نرم افزارها، برنامه ها و آنتی ویروس های خود را بروز رسانی کنید.
۵. به طور منظم از اطلاعات حیاتی خود بر روی سیستم ها و پوشه های به اشتراک گذاشته نسخه پشتیبان خارج از شبکه و سیستم تحت شبکه تهیه کنید چرا که باج افزار ها می توانند حتی فایل های مبتنی بر شبکه و داخل فولدرهای اشتراکی را نیز آلوده کنند.