بد افزار Ransomware (باج افزار) یا ویروس باج گیر چیست ؟

باج افزار یا ویروس باجگیر نوعی بد افزار است که به طراحانش این امکان را می دهد تا بتوانند از طریق کنترل از راه دور، کامپیوتر قربانی و سیستم آلوده را قفل کنند و فایل های به اشتراک گذاشته شده را رمزنگاری Encrypt کند به طوری که کاربر نتواند از سیستم خود استفاده کند.

بعد از آلوده شدن سیستم کامپیوتری کاربر به ویروس باجگیرRansomware ، یک پنجره پاپ آپ روی کامپیوتر شخص نمایان می شود و اخطاری به این شرح می دهد که قفل فایل های سیستم تان باز نمی شود تا زمانی که هزینه ای را برای باز کردن آن نپردازید.

چگونه کاربران شبکه و کامپیوترها درگیر باج افزار Ransomware می شوند؟

باز کردن یک ایمیل حاوی ضمیمه مخرب و آلوده

کلیک روی لینک های ویران گری که در ایمیل، شبکه های اجتماعی یا سایت ها قرار دارد.

بازدید از سایت های مشکوک که اغلب دارای ماهیت مستهجن هستند.

باز کردن فایل های آلوده به ویروس های باجگیرRansomware

باز کردن ماکرو های فاسد در اسناد برنامه (مثل واژه پرداز ها و صفحه گستر ها)

اتصال به دستگاه های جانبی usb مثلMemory، هارد اکسترنال، Mp3 Playerو...

راه های جلوگیری از ورود باج افزارRansomware

هیچ گاه به ایمیل های ناشناس پاسخ ندهید یا ایمیل هایی را که در قسمت Spam ایمیل تان قرار دارد را باز نکنید.

تنها از وب سایت های امن یا وب سایت هایی که می شناسید استفاده کنید.

قبل از آنلاین شدن، از وجود آنتی ویروس و دیوار آتش مؤثر و به روز روی کامپیوتر خود مطمئن شوید.

به طور منظم از اطلاعات خود نسخه پشتیبان تهیه کنید در خارج از محیط شبکه و سیستم کامپیوتری نگهداری نمایید.

اگر درگیر باج افزار Ransomware شدیم چه کار کنیم؟

برای حذف باج افزار یا دیگر نرم افزارهای مخرب که ممکن است روی کامپیوتر شما نصب شده باشد، یک Scan کامل بوسیله آنتی ویروس اصل، با یک راه حل Solution امنیتی مناسب و به روز انجام دهید

اگر کامپیوتر شما از طریق باج افزار قفل شده باشد، حتماً برای مشاوره و راهنمایی از یک منبع قابل اعتماد استفاده کنید و به هیچ وجه پول را واریز نکنید چرا که حتی اگر آن ها قفل کامپیوتر شما را باز کنند، پس از مدتی دوباره از شما باج گیری و کامپیوتر شما را قفل می کنند. بنابراین به دنبال یک راه قطعی و مطمئن باشید.

فعلا تنها راه مقابله با ویروس های باجگیر و نرم افزارهای مخرب RanSomware داشتن بک آپ Backup منظم روزانه یا هفتگی و گرفتن نسخه پشتیبان مناسب از داده های کامپیوتری و نگهداری این اطلاعات در خارج از شبکه و سرور می باشد.

اگر سیستم شبکه تان و فایل های شیر Share Files شرکت شما به ویروس باج گیر Ransomware آلوده شده است، دو راهکار وجود دارد:

راه حل اول:

بررسی فایل های آلوده برای مشخص کردن نام باج افزار و پیدا کردن مکانیزم رمزنگاری و عملکرد ویروس باجگیر مربوطه و در نهایت پیدا کردن ابزار رمزگشایی Decrypt برای بازیابی فایل های آلوده.

راه حل دوم:

پاکسازی بستر شبکه و سرورها و کامپیوترها از دست باج افزار RansomWare و استفاده از نسخه های پشتیبان (در صورت وجود) و راه اندازی مجدد سرویس های شبکه.