بدافزارهای باج گیر! پیشگیری یا ...؟

بدافزارهای باج گیر بر خلاف سایر نمونه‌ها، عملا با سیستم‌عامل کاری نداشته و هدف اصلی آن‌ها، فایل‌ها و اطلاعات شخصی کاربران است که با رمزگذاری کردن این فایل‌ها از کاربر می‌خواهند برای بازگرداندن اطلاعات خود، مبالغی را که بعضا تا هزاران دلار افزایش می‌یابد پرداخت کنند. از همین روی به آن‌ها نام باج‌گیر اطلاق می‌شود.

وقتی سیستم قربانی به این بدافزار آلوده می‌شود، در ابتدا تمامی فایل‌های سیستم اسکن شده و رمز گذاری می‌شوند، به گونه‌ای که دیگر قابل دسترسی نیستند. در نسخه‌های جدید یک پسوند اتفاقی برای فایل ها انتخاب می‌شود .بعد از آن یک صفحه به شما نمایش داده می‌شود که شما را از رمز شدن فایل‌ها آگاه کرده و دستورالعملی برای پرداخت مبلغ جهت بازگرداندن آن‌ها به شما ارائه می‌کند.

این بدافزار حتی به کاربر اجازه می‌دهد برای اطمینان چند مورد از فایل‌های رمز شده را رمزگشایی کند که این کار برای آن است که کاربر متوجه شود در صورت پرداخت مبلغ، فایل‌های خود را بازپس خواهد گرفت و از این طریق برای پرداخت مبلغ تشویق شود .

راه های ورود بد افزار های باجگیر به رایانه و شبکه محلی:

۱) باز کردن یک ایمیل دارای پیوست یا ضمیمه مشکوک و مخرب.

۲) کلیک روی لینک های مخرب که در ایمیل، شبکه های اجتماعی یا سایت ها قرار دارند.

۳) بازدید از سایت های مخرب که اغلب دارای ماهیت مستهجن هستند.

۴) دانلود فایل‌های مشکوک، کرک‌ها، نرم‌افزارهای اجرایی و آلوده و عدم استفاده از نسخه ی اصلی نرم افزار ها

۵) باز کردن ماکروهای فاسد در اسناد برنامه (مثل واژه پردازها word و صفحه گسترهاexcel)

۶) اتصال به دستگاه‌های جانبی usb مثل memory ، هارد اکسترنال ، mp3 playerکه محتویات آنها مطمئن نیستند و یا به سیستمهای عمومی متصل شده اند.

جلوگیری از ورود بدافزار یا باج افزار:

۱) وجود آنتی‌ویروس و بروز بودن آنها بسیار مهم است

۲) هیچگاه به ایمیل های با محتوای نامعلوم و یا ایمیل هایی که در junk و spamقرار می گیرند، پاسخ ندهید.

۳) تنها از وب سایت‌های امن یا وب سایت‌هایی که می‌شناسید استفاده نمایید.

۴) به طور منظم از اطلاعات مهم خود نسخه پشتیبان تهیه کنید و خارج از سیستم نگه داری فرمایید.

چنانچه سیستم شما به این بدافزار آلوده شد چه می‌توان کرد؟

فوری‌ترین کار اسکن سیستم با یک آنتی‌ویروس مطمئن و به‌روز است. متأسفانه اغلب کاربران تا هنگامی که با صفحه درخواست پول مواجه نشده‌اند، متوجه حضور این بدافزار در سیستم خود نمی‌شوند. آنتی ویروس قادر به حذف بدافزار است و در نتیجه با شروع دوباره سیستم این بدافزار فعال نخواهد شد .

متأسفانه هیچ راهی برای بازگرداندن فایل‌های رمز شده وجود ندارد؛ چنانچه گزارش مرکز ماهر نیز به آن اشاره کرده است. همچنین سایر ابزارهای رمزگشایی که از سوی شرکت‌های امنیتی برای مقابله با باج‌گیرها عرضه شده در خصوص برخی از این گونه بدافزارها کاربردی ندارد. تنها راه، بازگرداندن فایل‌ها یا Restoreکردن آن‌هاست؛ آن هم در صورتی که پیش از این از آن‌ها نسخه پشتیبان یا Backup تهیه کرده باشید .

با وجود نصب و بروز بودن آنتی‌ویروس، گاهی اوقات سیستم های رایانه ای به بدافزارهای باج گیر آلوده می شوند که کلیه فایلهای داخل رایانه را رمزنگاری می‌نماید و پس از آلوده کردن سیستم قربانی ، باج افزار به سرعت به سایر سیستم های شبکه نیز منتقل می شود.

در صورت مشاهده هر گونه مورد مشکوک ، مراتب را سریعا به اداره فناوری اطلاعات و همچنین حراست دانشگاه اعلام نمایید.

اقتصاد مقاومتی، اقدام و عمل

دانشگاه پیام نور
استان خراسان جنوبی

بدافزارهای باج گیر

پیشگیری یا ...!

تهیه شده توسط:

شورای IT حراست دانشگاه

رایانامه: H561@pnu.ac.ir

تلفکس: ۰۵۶-۳۲۲۰۲۲۷۱

بهار ۹۵