عنوان کارگاه : **پیاده سازی حملات باج افزاری و راهکارهای مقابله**

باج افزار (**Ransomware**) چیست ؟

باج افزار 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 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 می دهند که قربانی بتواند رمز را وارد و پول را پرداخت کند.

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

- باز کردن یک ایمیل حاوی ضمیمه مخرب.
- کلیک روی لینک های مخرب که در ایمیل، شبکه های اجتماعی یا سایت ها قرار دارد .
- بازدید از سایت های مخرب که اغلب دارای ماهیت مستهجن هستند.
- باز کردن فایل های آلوده از فایل دیجیتال شرکت های حمل و نقل منتنی بر وب.
- باز کردن ماکرو های فاسد در اسناد برنامه (مثل واژه پرداز ها و صفحه کستر ها).
- اتصال به دستگاه های جانبی usb مثل memory ، هارد اکسترنال ، mp3 player و ...
- استفاده از سی دی یا فلاپی های آلوده در کامپیوتر خود.
- عدم به روز رسانی سیستم عامل و وجود حفره های امنیتی در سیستم (... , RDP)

جلوگیری از ورود باج افزار

- هیچ گاه به ایمیل های ناشناس پاسخ ندهید یا ایمیل هایی را که در قسمت spam ایمیلتان 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 چرا که برخی از باج افزار ها می توانند حتی فایل های مبتنی برابر ذخیره سازی را نیز آلوده کنند .

سرفصل های کارگاه باج افزار

در این کارگاه ابتدا توضیحات جامع و مختصری در مورد باج افزارها و نحوه ورود باج افزارها به مدعوین داده میشود.

کار عملی:

در مرحله بعد به صورت عملی و واقعی یک حمله بر روی سیستم های مستقر در آزمایشگاه انجام شده و از طریق نرم افزارهای مانیتورینگ مراحل انجام حمله نمایش داده شده و حضار با عملکرد واقعی باج افزار آشنا می شوند.

سپس با استفاده از نرم افزارهای مانتیورینگ مراحل حمله تجزیه و تحلیل می شود.

و در نهایت به صورت عملی راه های برقراری امنیت و روش های حفاظت از اطلاعات به مدعوین آموزش داده می شود.

و در پایان به حضار آموزش داده می شود که در صورت مواجهه با یک حمله باج افزاری چه عکس العملی نشان داده و برای بازیابی اطلاعات حود چه کاری می توانند انجام دهند.