برنامه های مخرب که امنیت اطلاعات کاربران را تهدید می‌کنند؟

به طور کلی چیزهایی که افراد باید برای امنیت شبکه و تجهیزات در حال استفاده نگران‌شان باشید، موارد زیر هستند:

تروجان

تروجان‌ها شاید در نگاه اول، هیچ فرقی با یک برنامه معمولی کامپیوتر نداشته باشند؛ اما حقیقت این است که آن‌ها می‌توانند بدون اجازهٔ شما، فایل‌ها را حذف کنند، بدافزارهای مخفی شده در رایانه‌تان را فعال کنند و کارایی رایانه و شبکه را هم کاهش دهند.

ویروس

یک فایل مخرب که می‌تواند بدون اطلاع شما تکثیر شود، فایل‌های‌تان را آلوده کرده و حتی آنها را به دستگاه دیگران ارسال کند.

کِرم‌ها

کرم‌ها (WORMS) وارد شبکه شما شده، پهنای باند آن را مصرف می‌کنند و باعث کاهش کارایی شبکه می‌شوند.

نرم افزارهای جاسوسی

نرم‌افزارهای جاسوسی دقیقا مثل یک جاسوس در شبکه عمل کرده و هر برنامه و فایلی را که بخواهند، بدون اطلاع شما برای دیگران ارسال می‌کند.

ADWARE

این‌ها یک سری برنامه‌های جاسوسی تبلیغاتی هستند. درواقع این برنامه‌ها، رفتارهای شما را بررسی کرده و پس از مدتی، نزدیک‌ترین تبلیغات اینترنتی مشابه با سلایق و رفتارتان را به شکل پاپ‌آپ روی رایانه‌تان نمایش می‌دهند.

باج افزارها

باج افزارها همان‌طور که از اسم‌شان هم پیداست، به دنبال گرفتن باج از شما هستند! صاحبان آن‌ها با کدگذاری فایل‌های شبکه یا قطع دسترسی کاربر به رایانه، از او درخواست باج دادن در ازای برگشت شرایط به حالت عادی را می‌کنند.

راه های مقابله با تروجان ها چیست ؟

در ابتدا با نصب نرم افزار ضد بدافزارهای مؤثر ، می توانید از دستگاه های خود از جمله رایانه های شخصی ، لپ تاپ ، مک ، تبلت و تلفن های هوشمند – در برابر تروجان دفاع کنید. یک راه حل سختگیرانه ضد بدافزار استفاده از آنتی ویروس می تواند حملات تروجان را روی رایانه شما تشخیص داده و از آن جلوگیری می کند .

زمانیکه یک تروجان فعال می شود شروع به انجام دادن انواع و اقسام تخریب ها از جمله پاک کردن اطلاعات و فایل ها ، جایگزین کردن داده ها بر روی کامپیوتر آلوده و در نهایت جاسوسی از جمله مواردی است که تروجان ها می توانند پس از آلودگی سیستم قربانی انجام بدهند . قطعا موارد دیگری از جمله به سرقت بردن اطلاعات و جاسوسی و ثبت و ضبط کلمه های تایپ شده روی سیستم و سرقت اطلاعات کارت های بانکی از دیگر فعالیت های مخرب یک تروجان است اما از چه روش هایی می توان با تروجان ها مقابله کنیم ؟ روشهای مقابله با تروجان را بصورت کلی به موارد زیر تقسیم بندی می کنیم:

1. به هیچ عنوان پیوست های ایمیلی که ارسال کننده آنها ناشناس است را باز نکنید
2. کلیه پورت های بلااستفاده را بر روی فایروال خودتان مسدود کنید
3. هیچ برنامه ای از پیام رسان ها دانلود و نصب نکنید
4. تنظیمات پیشفرض دستگاه ها و سیستم عامل ها را تغییر بدهید
5. پروتکل ها و سرویس های بلااستفاده در سیستم را حذف کنید
6. دائما ترافیک شبکه و سیستم ها را در شبکه مانیتور و موارد مشکوک را بررسی کنید
7. از هیچ منبع غیر معتبری نرم افزار دانلود و نصب نکنید
8. همیشه سیستم عامل ها و برنامه ها را به آخرین بسته های به روزرسانی مجهز کنید
9. CDو Flash و ابزارهای جانبی ذخیره اطلاعات را قبل از استفاده اسکن امنیتی کنید
10. از نصب شدن نرم افزارها بصورت غیرمجاز در شبکه توسط کاربران عادی جلوگیری کنید
11. هیچوقت بدون اطلاع اسکریپت یا دستوری را اجرا نکنید

سخن پایانی:

در هفته آینده با سایر موارد مخرب بحث و راهکارهای مقابله با آنها را بحث خواهیم کرد