نشانه های ویروسی شدن رایانه
و راه مقابله با آن

مقدمه :

به یک ویروس بیولوژیک فکر کنید، از آن دسته نمونه‌هایی که وارد بدن شده و موجب بیماری می‌شوند و با آلوده کردن شما اجازه نمی‌دهند به درستی فعالیت روزمره‌تان را ادامه دهید؛ **ویروس‌های کامپیوتری** نیز تا حد زیادی مشابه ویروس‌های بیولوژیک‌اند و برنامه‌ها را تحت تاثیر قرار داده و باعث می‌شوند که کامپیوتر نتواند به درستی کار کند یا حتی آن را به طور کامل از کار می‌اندازند.

ویروس چطور میزبانش را پیدا می‌کند؟

حتی اگر یک کاربر کامپیوتر کاملا جوانب امنیتی را رعایت کند، باز هم این امکان وجود دارد که ویروس‌ها از طریق فعالیت‌های طبیعی در فضای مجازی خود را وارد کامپیوتر کنند مثل **فرستادن موسیقی، فایل یا عکس به کاربران دیگر، ورود به یک وب سایت آلوده، باز کردن یک هرزنامه یا فایل ضمیمه شده به یک ایمیل، دانلود کردن بازی، نوار ابزار، برنامه یا هر اپلیکیشن رایگان دیگر** و نصب برنامه‌ای که می‌توانند به اطلاعات رایانه دسترسی داشته باشد.بعضی از ویروس‌ها طراحی شده‌اند تا با آسیب رساندن به برنامه‌ها، پاک کردن فایل‌ها و یا فرمت کردن هارد دیسک به کامپیوتر آسیب برسانند. برخی دیگر تنها وارد جریان ترافیک اینترنتی می‌شوند و اتصال به اینترنت و انجام فعالیت‌های مجازی را غیر ممکن می‌کنند. بعضی ویروس‌های کم‌خطرتر نیز تنها کارکرد طبیعی کامپیوتر را مختل کرده و یا حافظه کامپیوتر را از بین می‌برند و یا اینکه چندین مشکل کوچک رایانه‌ای به وجود می‌آورند.

نشانه‌های ویروس کامپیوتری چیست؟

اگر یک کامپیوتر مورد حمله ویروس قرار گرفته باشد، می‌توان با توجه به نشانه‌های زیر متوجه وجود یک بدافزار در رایانه شد؛ **کندی در عملکرد کامپیوتر، عملکرد نامنظم کامپیوتر، از بین رفتن برخی اطلاعات به صورت ناگهانی.**واژه «ویروس کامپیوتری» به عنوان اصطلاحی برای نامیدن تمام انواع بدافزار به کار گرفته می‌شود؛ بد افزارها شامل **ویروس‌های کامپیوتری، کرم کامپیوتر، اسب تروا ، اکثر روت‌کیت‌ها، نرم افزارهای جاسوسی، ابزارهای تبلیغاتی نامناسب** و بسیاری از نرم افزارهای ناخواسته دیگر می‌شود که می‌توان نام ویروس را بر آن‌ها گذاشت.ماهیت ویروس‌های کامپیوتری گاهی با

آنچه با نام کرم‌های کامپیوتر یا بدافزار اسب تروا شناخته می‌شود اشتباه گرفته می‌شوند در حالیکه این دو بدافزار کاملا متفاوت از یکدیگرند. یک کرم کامپیوتری می‌تواند به سیستم امنیتی آسیب وارد کرده و از طریق کامپیوتر میزبان و اتصال به اینترنت به صورت اتوماتیک به دیگر کامپیوترها ورود پیدا کند درحالیکه بدافزار اسب تروا در ظاهر بی‌خطر به نظر می‌رسد اما می‌تواند به صورت پنهانی مخرب باشد.برخی ویروس‌ها و بدافزارها نشانه‌هایی را روی کامپیوتر آلوده از خود به جای می گذارند که به راحتی قابل تشخیص است اما بسیاری از آنها به صورت پنهانی عمل می‌کنند و هیچ اثر مشکوکی از خود به جای نمی گذارند تا توجهی را به سمت خود جلب نکنند. برخی ویروس‌ها نیز تنها از فضای کامپیوتر میزبان استفاده می‌کنند تا بازتولید شوند و سپس تمام حجم کامپیوتر آلوده را فرابگیرند.

بدافزار اسب تروا :

اسب تروا ابزاری فریب‌دهنده است که در نگاه اول کاربر را ترغیب به استفاده می‌کند اما پس از آنکه شروع به کار می‌کند می‌تواند کامپیوتر میزبان را آلوده کند . تفاوت مهم بین اسب تروا و برنامه‌های حقیقی و ویروس‌ها این است که این بدافزار در کامپیوتر میزبان تکثیر نمی‌شود. اسب تروا شامل کدهای مخربی می‌شود که وقتی وارد عمل می‌شوند می‌توانند باعث از بین رفتن و یا حتی دزدیده شدن اطلاعات شوند. برای اینکه یک بدافزار اسب تروا بتواند خود را گسترش داده و وارد کامپیوتر میزبان شود حتما باید به این کامپیوترهای مورد هدف از سوی کاربر دعوت شود به این صورت که کاربر ایمیلی را که شامل یک فایل ضمیمه می شود باز می‌کند و یا برنامه‌ای را از طریق اینترنت دانلود کرده و در رایانه اش ران میکند.

کرم کامپیوتری :

کرم‌های کامپیوتری طراحی شده‌اند تا بتوانند با انتقال خود از یک کامپیوتر به کامپیوتری دیگر گسترش پیدا کنند بی‌آنکه از فایلهای کامپیوتر میزبان استفاده کنند .کرم‌ها بر خلاف ویروس‌ها برای تکثیر نیازی به دسترسی به فایل‌های کامپیوتر میزبان ندارند. اگرچه بیشتر کرم‌های کامپیوتری در فایل‌های کامپیوتر میزبان اغلب فایل های ورد و اکسل وجود دارند اما بین نحوه استفاده کرم‌ها و ویروس‌ها از کامپیوتر میزبان تفاوت‌های عمده‌ای وجود دارد.معمولا کرم‌های کامپیوتری فایل‌هایی را که از قبل آلوده شده است، رها می‌کنند .کرم‌های کامپیوتری از طریق انتقال یک فایل آلوده کامل به کامپیوتر میزبان بعدی خود وارد می‌شوند بنابراین کل فایل آلوده و اطلاعات داخل آن به عنوان «کرم» شناخته می‌شود.

ترس افزارها

ترس افزارها در واقع نوع دیگری از ویروس Hoex یا جعلی هستند که در زمان باز کردن یک وب سایت به صورت اخطار روی صفحه کامپیوتر نشان داده می‌شوند و به کاربر اخطار می دهند که کامپیوترش آلوده به نوعی ویروس شده است. اما اگر نگاه نزدیکتری به این اخطار کنید می‌توانید متوجه شوید که این پیام اخطار ربطی به برنامه آنتی ویروس ندارد و اخطاری از سوی ویندوز کامپیوتر است.

از کامپیوترتان محافظت کنید

این ها چند راه حل برای محافظت از کامپیوتر در مقابل انواع بد افزارها هستند.

فایروال (دیوار آتش):

برنامه فایروال می‌تواند کامپیوتر را در مقابل ورود هکرها و نرمافزارها مخرب محافظت کند. فایروال نرمافزار یا سخت افزاری است که اطلاعاتی را که از طریق اینترنت یا شبکه وارد کامپیوتر می‌شوند، پیش از ورود چک می‌کند و بر اساس تنظیماتش آنها را یا رد می‌کند و یا به این اطلاعات اجازه ورود می‌دهد. به این ترتیب فایروال می‌تواند جلوی ورود هکرها و بدافزارها را بگیرد. فایر وال روی ویندوز نصب می‌شود و به طور خودکار با بالا مدن ویندوز شروع به کار می‌کند.اگر یک برنامه ای مانند یک بازی اینترنتی یا یک سیستم مسیجینگ را روی کامپیوترتان باز کنید و این برنامه بخواهد با اتصال به اینترنت اطلاعاتی را به دست آورد، فایروال از شما می‌پرسد که آیا مایل به قطع این ارتباط هستید یا خیر. اگر شما اجازه برقراری این ارتباط را برای بار اول به برنامه مورد نظر بدهید فایر وال در آینده در مورد برقراری ارتباط اینترنتی جهت دریافت اطلاعات دیگر از شما سوالی نمی پرسد و به صورت خودکار اجازه برقراری چنین ارتباطی را به برنامه مذکور می دهد.

آنتی ویروس :

آنتی ویروس برنامه‌ای است که ای‌میل و فایلهای دیگر کاربر را برای پیدا کردن ویروس، کرم یا اسب تروا جست‌وجو می‌کند. این برنامه اگر بتواند یکی از موارد خطرناک بدافزار را پیدا کند، آن را قرنطینه کرده یا قبل از آنکه بتواند آسیبی به کامپیوتر وارد کند آن را پاک خواهد کرد.ویندوز به طور خودکار برنامه آنتی ویروسی را روی خود ندارد اما شرکت سازنده کامپیوتر ممکن است یکی از این برنامه‌های آنتی ویروس را روی ویندوز نصب کرده باشد .اما اگر هیچ آنتی ویروسی روی سیستم کامپیوتر شما نصب نشده است، راه‌های زیادی برای پیدا کردن و نصب کردن یکی از آن ها وجود دارد .مایکروسافت برنامه‌هایی را به عنوان برنامه

ضروری امنیتی به شما پیشنهاد می‌دهد که می‌توانید آن را از وب‌سایت Microsoft Security Essentials به صورت رایگان دانلود کنید.

برنامه حفاظت از جاسوس افزار:

جاسوس‌افزار یا نرم‌افزار جاسوسی بدافزاری است که اطلاعات کاربر را جمع آوری کرده و سپس بخش تنظیمات کامپیوتر را بدون رضایت کاربر تغییر می‌دهد. برای مثال جاسوس افزارها می‌توانند نوار ابزار، لینک را روی کامپیوتر میزبان نصب کنند، صفحه اصلی مرورگر را تغییر دهند، یا پیام‌های تبلیغاتی را به شما نشان دهند.برخی جاسوافزارها نیز بی آنکه رد پایی از خود به جا بگذارند تنها اطلاعات مهم و سری شما مثل وب سایت‌هایی که اخیرا باز کرده‌اید یا افرادی که به تازگی به آنها پیام داده‌اید را جمع‌آوری می‌کنند. بیشتر نرم‌افزارهای جاسوسی از طریق برنامه رایگانی که دانلود شده است به کامپیوتر میزبان راه پیدا می‌کنند در حالیکه برخی دیگر ممکن است تنها با باز کردن آدرس یک وب‌سایت وارد کامپیوتر مورد نظرشان شوند.برای محافظت از کامپیوترتان در مقابل جاسوس افزارها کافی است یک برنامه ضد جاسوس‌افزار نصب کنید. ورژن‌های جدید ویندوز به یک آنتی جاسوس افزار مجهزاند که به طور خود کار با بالا آمدن ویندوز به کارمی‌افتد. این برنامه که Windows Defender نام دارد زمانیکه یک جاسوس‌افزار قصد ورود به کامپیوترتان را دارد به شما هشدار می‌دهد و همچنین کامپیوتر را برای یافتن چنین برنامه‌های بازرسی کرده و در صورت برخورد با نمونه‌ای از این بدافزار آن را پاک می‌کند.

نصب آخرین ورژن مرورگر :

در بیشتر مواقع جدیدترین نسخه‌های مرورگر شامل برخی اصلاحات امنیتی می‌شوند که می‌تواند از امنیت و حریم شخصی کاربر زمانی که به اینترنت متصل شده است محافظت کند.

تهیه کننده : **عدنان بوعذار**

دبیر گروه کامپیوتر دبیرستان استعدادهای درخشان شهید بهشتی اهواز (دوره یکم)