زمان تقریبی مطالعه: ۷ دقیقه

ویروس‌ها، کرم‌ها و تروجان‌ها چه هستند؟

ویروس‌ها، کرم‌ها و تروجان‌ها برنامه‌های مخربی هستند که می‌توانند خطراتی جدی برای کامپیوتر و اطلاعات شما ایجاد کنند. این نرم‌افزارهای آلودگی‌زا، می‌توانند سرعت اینترنت شما را کاهش دهند و حتی ممکن است از کامپیوتر شما برای پخش خود به دوستان، آشنایان و همکاران استفاده کنند و در آدرس‌های مجازی باقی بمانند. خبر خوب این است که با رعایت برخی تدابیر ساده، احتمال قربانی‌شدن شما به حداقل می‌رسد. پیشگیری از جانب شما می‌تواند خانواده‌تان را نیز در امان نگه دارد. با ما همراه باشید تا درباره مشخصات و تفاوت‌های ویروس‌ها، کرم‌ها و تروجان‌ها بیشتر بدانید

ویروس چیست؟

ویروس یک تکه کد کامپیوتری است که به یک برنامه یا فایل وابسته است و بنابراین می‌تواند از کامپیوتری به کامپیوتر دیگر منتشر شود. ویروس‌ها می‌توانند خطراتی جدی برای نرم‌افزار، سخت‌افزار و فایل‌های شما ایجاد کنند.

این کدها به طوری نوشته شده‌اند که هدف آن‌ها تکرار خودشان است. یک ویروس برای انتشار از یک کامپیوتر به کامپیوتر دیگر تلاش می‌کند و معمولاً وابسته به یک برنامه خاص است. این ویروس‌ها ممکن است برای سخت‌افزار، نرم‌افزار یا اطلاعات شما خطرناک باشند. دامنه تاثیرگذاری ویروس‌های انسان‌ساز از چند ساعت تا بی‌نهایت متغیر است، در حالی که دامنه ویروس‌های کامپیوتری می‌تواند از آزاردهنده تا کاملاً مخرب متفاوت باشد.

نکته‌ای که باید به خاطر داشته باشید این است که یک ویروس واقعی بدون اقدام انسان، مانند اشتراک‌گذاری فایل یا ارسال ایمیل، قادر به حرکت و گسترش نیست.

کرم چیست؟

یک کرم، مشابه ویروس، برای کپی خود از یک کامپیوتر به دیگری طراحی شده است، اما به‌طور خودکار کنترل کامپیوتر را به‌دست می‌گیرد و می‌تواند فایل‌ها و اطلاعات را منتقل کند. زمانی که یک کرم در سیستم شما وجود داشته باشد، می‌تواند به تنهایی حرکت کند و گسترش یابد.

خطر بزرگ کرم‌ها توانایی آن‌ها در ایجاد ترافیک سنگین شبکه است. به عنوان مثال، یک کرم می‌تواند کپی‌های خود را برای هر شخصی که در آدرس ایمیل شما ثبت شده، ارسال کند و سپس کامپیوترهای آن‌ها نیز همین عمل را انجام خواهند داد. این فرآیند می‌تواند موجب کاهش سرعت شبکه و اینترنت شود. هنگام ظهور کرم‌های جدید، آن‌ها به سرعت پخش می‌شوند و ممکن است باعث تاخیر در دسترسی به صفحات وب شوند.

کرم‌ها به طور کلی بدون نیاز به اقدام کاربر منتشر می‌شوند و کپی‌های خود را در سراسر شبکه‌ها توزیع می‌کنند.

این نرم‌افزارهای مخرب می‌توانند حافظه یا پهنای باند شبکه را مصرف کرده و در نتیجه، پاسخ‌دهی کامپیوتر را متوقف کنند. از آن‌جایی که کرم‌ها برای حرکت نیاز به یک برنامه یا فایل خاص ندارند، می‌توانند در داخل سیستم شما نفوذ کنند و اجازه دهند که هرکس دیگر کنترل سیستم شما را در دست بگیرد. به تازگی، نمونه‌های کرم‌ها از قبیل «سایزر وبلاستراست» شناسایی شده‌اند.

تروجان چیست؟

تروجان‌ها نرم‌افزارهایی هستند که به‌ظاهر مفید به نظر می‌رسند، اما در واقع امنیت شما را تهدید می‌کنند. این نام به‌خوبی از افسانه اسب تروjan گرفته شده است؛ جایی که این اسب به عنوان هدیه‌ای به شهر تروی وارد شد و سربازان پنهانی در آن حضور داشتند. در دنیای امروز، تروجان‌ها معمولاً از طریق پیام‌های ایمیلی که ادعا می‌کنند جزئی از بروزرسانی‌های امنیتی مایکروسافت هستند، منتشر می‌شوند. این نرم‌افزارها می‌توانند به راحتی به سیستم شما نفوذ کرده و عملکرد آنتی‌ویروس و دیوار آتش شما را مختل کنند.

تروجان‌ها به کاربران القا می‌کنند که این برنامه‌ها از منابع معتبر هستند، به همین دلیل کاربران به سادگی آن‌ها را باز می‌کنند و در نتیجه به سرعت پخش می‌شوند. برای حفاظت بهتر کاربران، مایکروسافت به‌طور مرتب بیانیه‌های امنیتی از طریق ایمیل ارسال می‌کند، اما این بیانیه‌ها هرگز شامل پیوست‌های مشکوک نمی‌شوند.

تروجان‌ها همچنین می‌توانند بخشی از نرم‌افزارهایی باشند که شما به‌صورت رایگان دانلود می‌کنید؛ لذا هرگز نرم‌افزاری را از منابع نامعتبر دانلود نکنید. اطمینان حاصل کنید که همیشه به‌روزرسانی‌های مایکروسافت را از وب‌سایت‌های معتبر دریافت کنید.

محافظت در برابر تهدیدات سایبری

واقعاً همه ویروس‌ها و بسیاری از کرم‌ها نمی‌توانند منتشر شوند مگر اینکه شما برنامه آلوده‌ای را باز یا اجرا کنید. بسیاری از این ویروس‌های خطرناک عمدتاً از طریق پیوست‌های ایمیلی که همراه با پیام‌های ایمیل ارسال شده، منتشر می‌شوند. معمولاً شما می‌توانید زمانی که ایمیل شما شامل پیوست باشد، متوجه شوید، چون آیکون کلیپ به شما نشان می‌دهد که متعلقات وجود دارند.

عکس‌ها، نامه‌های نوشته شده در Word مایکروسافت و حتی صفحات گسترده Excel تنها چند نوع از فایل‌هایی هستند که ممکن است هر روز از طریق ایمیل دریافت کنید. ویروس‌ها زمانی شروع به کار می‌کنند که شما پیوست فایل را باز کنید. اگر پیام ایمیلی از کسی که نمی‌شناسید با پیوست دریافت کردید، باید فوراً آن را حذف کنید. متأسفانه، شما از پیوست‌های ایمیل افرادی که می‌شناسید نیز نمی‌توانید ایمن باشید. ویروس‌ها و کرم‌ها قابلیت دزدیدن اطلاعات از برنامه‌های ایمیل را دارند و خودشان را به تمامی آدرس‌های ثبت شده ارسال می‌کنند.

بنابراین، اگر ایمیلی از کسی با پیامی که نمی‌فهمید یا فایلی که منتظر آن نبودید دریافت کردید، همواره با آن شخص تماس بگیرید و محتویات پیوست را تأیید کنید پیش از اینکه آن را باز کنید. ویروس‌های دیگر می‌توانند از طریق

برنامه‌های دانلود شده از اینترنت یا دیسکت‌های پاک‌کننده‌ای که از دوستان قرض می‌گیرید یا از فروشگاه خریداری می‌کنید، منتشر شوند. این‌ها رایج‌ترین راه‌های منقبض کردن ویروس‌های کامپیوتری هستند. اکثر مردم از طریق باز کردن و اجرای پیوست‌های ایمیل ناشناس آلوده می‌شوند.

چطور می‌توان گفت آیا کرم یا ویروس دیگری داریم؟

کامپیوتر شما ممکن است کند شود؛ یا ناگهان خاموش و دوباره راه‌اندازی شود. تمام این علائم میتواند نشان‌دهنده آلودگی کامپیوتر شما باشد، هرچند که ممکن است ناشی از برنامه‌های نرم‌افزاری و سخت‌افزاری باشند که هیچ ارتباطی با ویروس ندارند. برخی از ویروس‌ها قابلیت تغییر آدرس ایمیل را دارند. مگر اینکه شما نرم‌افزار آنتی‌ویروس جدید را نصب کرده باشید، راه مطمئنی برای اینکه بدانید آیا ویروسی دارید یا نه، وجود ندارد. اگر شما نرم‌افزار آنتی‌ویروس ندارید یا علاقه‌ای به نصب انواع نرم‌افزار آنتی‌ویروس ندارید، به صفحه نرم‌افزار امنیتی ما سر بزنید.

مراحل بعدی: کاهش خطر ویروس شما

هیچ تضمینی وجود ندارد که کامپیوتر شما ۱۰۰٪ ایمن باشد. با این حال، شما می‌توانید امنیت کامپیوترتان را با استفاده از نرم‌افزارهای نگه‌دارنده جدید و نگه‌داشتن اشتراک نرم‌افزار آنتی‌ویروس بهبود ببخشید.

حفاظت از PC شما

برای کمک به امن بودن کامپیوترتان در برابر بلاستر و خطرات دیگر در این اینترنت، به دستورالعمل محافظ PC برای برقراری دیوار آتش و به‌روزرسانی نرم‌افزار و استفاده از نرم‌افزار آنتی‌ویروس به روز مراجعه کنید.

قبل از اینکه شما مراحل دیگر را طی کنید، مطمئن شوید که از فعالیت دیوار آتش برای کمک به حفاظت کامپیوترتان در برابر آلودگی مطمئن باشید. اگر شما یک دیوار آتش سخت‌افزاری دارید در خانه یا محل کار یا اگر از دیوار آتش ویندوز XP استفاده می‌کنید. برای دستورالعمل جامع نصب و فعال‌سازی دیوار آتش به راهنمای محافظ PC مراجعه کنید.

سوالات متداول:

سوال چه اقدامات دیگری می‌تواند امنیت من را افزایش دهد؟
پاسخ: استفاده از دیوار آتش، نصب نرم‌افزار آنتی‌ویروس و به‌روزرسانی منظم سیستم عامل می‌تواند به شدت

امنیت شما را بهبود بخشد.

سوال: آیا ایمیل‌های ناشناس خطری دارند؟
پاسخ: بله، باز کردن ایمیل‌های ناشناس می‌تواند به انتشار ویروس‌ها و کرم‌ها منجر شود.

برای حفاظت بهتر از اطلاعات خود، اکنون نرم‌افزار آنتی‌ویروس خود را به‌روز کنید و از ایمنی دستگاه‌های خود اطمینان حاصل کنید!