

10 ویروس کشنده را بشناسید



سال 1980 ویروس‌هایی ایجاد شدند که برحسب کارهایی که کاربران انجام می‌دادند، می‌توانستند نمونه مشابه خودشان را تکثیر کنند سپس به رایانه‌های دیگر انتقال دهند.

جام جم آنلاین: سال 1980 ویروس‌هایی ایجاد شدند که برحسب کارهایی که کاربران انجام می‌دادند، می‌توانستند نمونه مشابه خودشان را تکثیر کنند سپس به رایانه‌های دیگر انتقال دهند.

ویروس‌های رایانه‌ای را می‌توان به کابوس تشبیه کرد. بعضی از این ویروس‌ها کل اطلاعات موجود در رایانه را پاک می‌کنند، برخی باعث ایجاد ترافیک‌های سنگین چند ساعته در شبکه‌های اینترنتی می‌شوند و دسته‌ای هم با سرعت بسیار بالا می‌توانند ویروس‌های مشابه خودشان را ایجاد و به رایانه‌های دیگر ارسال کنند اگر تا به حال رایانه‌تان ویروس نگرفته است، بخت با شما یار بوده؛ ولی اگر برحسب اتفاق آلوده به ویروس شود ممکن است خسارت بسیار زیادی به شما تحمیل کند.

برای نمونه سال 2008 مبلغی بالغ بر 16 میلیارد تومان به کاربرانی که رایانه‌شان دچار ویروس شده بود، خسارت وارد شد البته ویروس‌ها یکی از خطرات احتمالی اتصال به اینترنت به حساب می‌آیند، این در حالی است که شما باید خطرات دیگری را هم هنگام آنلاین بودن در نظر داشته باشید.

اولین باری که ویروس‌های رایانه‌ای ایجاد شدند، به طور دقیق مشخص نیست. تنها در سال 1949 ایده وجود برنامه‌ای که بتواند به شکل خودکار خودش را کپی و به رایانه‌های دیگر ارسال کند، مطرح شد.

10 سال بعد از این تاریخ، اولین برنامه رایانه‌ای که هکرها طراحی کرده بودند، در اینترنت انتشار یافت.

سال 1980 ویروس‌هایی ایجاد شدند که برحسب کارهایی که کاربران انجام می‌دادند، می‌توانستند نمونه مشابه خودشان را تکثیر کنند سپس به رایانه‌های دیگر انتقال دهند.

برای مثال هکرها ویروس‌ها را روی قسمتی از یک برنامه موجود در دیسکت ذخیره می‌کردند، پس از آن هر کسی که از آن دیسکت استفاده می‌کرد، ویروس سریعاً به رایانه‌اش منتقل می‌شد. امروزه هر وقت از ویروس بحث می‌شود، بیشتر کاربران یاد اینترنت می‌افتند.

بنا بر این احتمال این که ایمیل‌ها یا لینک‌هایی که از طریق اینترنت منتقل می‌شوند ویروسی باشند، زیاد است. در ادامه مطلب 10 نمونه از ویران‌کننده‌ترین ویروس‌ها را بررسی می‌کنیم.

1. Melissa: ویروس ملیسا را شخصی به نام دوید ال. اسمیت بر اساس برنامه ورد شرکت مایکروسافت طراحی کرده است. ملیسا از طریق ایمیل می‌تواند منتقل شود. به این ترتیب که کاربر، ایمیلی با این مضمون دریافت می‌کند: #171&اطلاعاتی که شما خواسته بودید، در این ایمیل است، لطفاً این ایمیل را به هیچ‌کس دیگری نشان ندهید.» پس از باز کردن این ایمیل، ویروس به شکل خودکار نمونه‌های مشابه خود را کپی می‌کند و به 50 نفر از آدرس‌هایی که در قسمت حافظه ایمیل‌تان ذخیره شده است، ارسال می‌کند.

2. یک سال پس از این که ملیسا در اینترنت غوغا به پا کرد، ویروس دیگری که بیشتر شبیه به کرم بود در فیلیپین طراحی شد. این کرم بدون نیاز به برنامه دیگری به شکل خودکار کرم‌های مشابه خود را تولید می‌کرد و نامش ایلو... بود. همانند ملیسا توسط ایمیل در تمام اینترنت گسترش پیدا کرد.

عنوان ایمیل هم #171& نام‌های از یکی از علاقه‌مندان شما « بود. با باز کردن ایمیل و دانلود attachment داخل ایمیل، این ویروس براهتی کپی می‌شد.

3. مدل سوم از ویروس‌ها که مانند ویروس‌های قبلی از طریق ایمیل به کاربر ارسال می‌شد Klez نام داشت. این ویروس بعد از باز کردن ایمیل با سرعت مدل مشابه خود را کپی، سپس مانند ملیسا به آدرس‌های موجود در حافظه ایمیل کاربر ایمیلی ارسال می‌کرد.

این ویروس به صورت‌های مختلفی مانند: کرم، تروجان و ویروس‌های عادی رایانه‌ای موجود بود. مدل‌های متفاوت این ویروس می‌توانستند آنتی‌ویروس شما را از کار بیندازد و نگذارد کاربر ویروس را پاک کند.

از دیگر کارهایی که این ویروس با آدرس‌های ایمیل شما می‌کند، انجام عمل spoofing بود. در حقیقت با اسپوفینگ شما ایمیل‌هایی از افراد ناشناس دریافت می‌کردید، در حالی که در قسمت فرستنده ایمیل نام یکی از دوستان‌تان قرار داشت.

4. چهارمین ویروس بسیار خطرناک موجود در اینترنت Code Red II و Code Red است. این دو ویروس سال 2001 طراحی شدند که سیستم‌عامل رایانه، بویژه ویندوز 2000 و NT را هدف می‌گرفت. با وارد شدن این ویروس به سیستم عامل، عمل buffer overflow اتفاق می‌افتاد.

با این کار، اطلاعات بسیار زیادی به حافظه راه می‌یافت و آن را اشباع می‌کرد و در نتیجه کاربر نمی‌توانست کارهای دیگری توسط رایانه‌اش انجام دهد.

5. نیمدا (Nimda) نوع دیگری از ویروس‌های اینترنتی سال 2001 بود، که تنها 22 دقیقه بعد از ورودش به اینترنت در رده اول قاتلان رایانه‌ای قرار گرفت. این ویروس برای آسیب زدن به سرورهای اینترنتی طراحی شده بود.

یکی از راه‌های وارد شدن این ویروس نیز به سیستم از طریق ایمیل بود. Nimda با ایجاد backdoor در سیستم عامل این امکان را برای هکر ایجاد می‌کرد که برایتی از طریق این راه به سیستم عامل کاربر وارد شود بنابراین هکر می‌توانست تغییرات مورد دلخواه خود را روی سیستم عامل کاربر ایجاد کند یا اطلاعات مورد نیاز خود را از آن بدزدد، که هر دوی این موارد جزو بزرگ‌ترین خطرات برای کاربر به حساب می‌آمدند.

6. SQL Slammer/Sapphire در حقیقت ویروسی است که برای شبکه‌های اینترنتی طراحی شده بود. این ویروس مانع انجام کار شرکت‌های بزرگ به شکل آنلاین می‌شد؛ برای همین هم خسارت هنگفتی در آن زمان به این شرکت‌ها وارد آمد.

7. مای دوم (MyDoom) نوع دیگری از انواع ویروس‌هاست که یکی از وظایف مخرب آن ایجاد backdoor در سیستم عامل است.

دومین عمل ویران‌کننده این ویروس انجام جستجو در جستجوگر و کپی تمام آدرس‌های موجود در مرورگر بود. مثلاً جستجوگر مانند گوگل میلیون‌ها تقاضا برای جستجو روی سایت خود دریافت می‌کرد و این کار سرعت جستجوگر را برای دریافت درخواست‌های جدید کاهش می‌داد و نمی‌توانست به جستجوهای کاربران حقیقی پاسخ دهد.

8. Sasser and Netsky هشتمین ویروس از سری قاتلان رایانه‌ای محسوب می‌شود، که هکر آن توسط پلیس دستگیر شد.

نحوه وارد شدن این ویروس به سیستم از طریق ایمیل نبود، بلکه این ویروس تنها از طریق تخریب رایانه و ارسال پیام به رایانه‌های دیگر، سیستم‌ها را تخریب می‌کرد. در حقیقت این ویروس مانع از خاموش شدن رایانه می‌شد و تنها راه خاموش کردن سیستم‌عاملی که این ویروس را به همراه داشت، قطع کابل برق آن بود.

9. Leap-A/Oompa-A تنها ویروسی بود که برای لپ‌تاپ‌های مک طراحی شده بود. این ویروس از برنامه iChat برای ارسال message به دیگر کاربران مک استفاده می‌کرد و مانند ویروس‌های دیگر با ورود به آی‌چت، فهرست اسامی دیگر کاربران را یادداشت می‌کرد.

پس از آن برای تمام آن افراد به صورت خودکار message می‌فرستاد. همراه این متن یک عکس ویروسی قرار داشت که با دانلود کردن آن، رایانه کاربر نیز آلوده به ویروس می‌شد.

10. استورم وارم به خاطر این که از طریق ایمیلی با این عنوان که æ171; نفر در توفان اروپا کشته شده‌اند» در اینترنت ارسال می‌شد، با این نام شناسایی شد.

پس از وارد شدن این ویروس به رایانه، به شکل Trojan horse وارد عمل می‌شد؛ یعنی کل سیستم‌عامل شما تحت کنترل هکر قرار می‌گرفت و این هکر بود که تعیین می‌کرد چه تغییرات و به چه شکل در رایانه ایجاد شود.

منبع: www.howStuffWorks.com - الهام اندرابی

