تعریف و راه‌های مقابله با

ویروس‌های کامپیوتری

نوشته: تابان خواجه نصیری
www.webfaqt.com

تابان خواجه‌نصیری- نویسنده، مترجم، روزنامه‌نگار، سخنران، طراح و مدیر چندین سایت اینترنتی ایرانی، متولد ۱۳۴۶ متاهل و ساکن تهران است- وی از سال ۱۳۶۸ با موسسات و شرکتهای انفورماتیکی متعددی در ایران در زمینه برگزاری سمینارهای آموزشی و مشاوره‌ای، بازاریابی و فروش نرم‌افزارهای کاربردی، نگارش و ترجمه فنی متون تخصصی و بعدها در خصوص ارائه‌ی استراتژیهای بازاریابی و تبلیغات اینترنتی، جذب مشتری از طریق اینترنت و طراحی و مدیریت سایتهای اینترنتی همکاری کرده است.

خواجه‌نصیری از سال ۱۳۷۳ به مطالعه، تحقیق، نگارش و ترجمه مقالاتی در زمینه کامپیوتر، اینترنت و فن‌آوری اطلاعات، ارتباطات در شبکه‌های اطلاع‌رسانی و اینترنت پرداخته است و همزمان با این فعالیتها، دانش نظری کسب شده را در سطوح عملی و تجربی به کار گرفته است. در طی این سالها، از وي مقالات متعددی در نشریات و مجلات ایرانی از جمله مجلات «علم الکترونیک و کامپیوتر»، «شبکه»، «کامیاب»، «آشیانه» و نیز سایتهای اینترنتی متعدد و معتبری در داخل و خارج از کشور منتشر و منعکس شده است.

برای طرح سوالات، نظرات و پیشنهادهای خود، با تابان خواجه‌نصیری می‌توانید از طریق فرمهای تماس بر روی سایت اینترنتی www.webfaqt.com و یا با شماره تلفن / فکس ٤١٠٤٥١٨ در تهران تماس حاصل نماید.

در طی یکی دو ماه گذشته، بسیاری از دوستانی که عضو خبرنامه‌های سایت webfaqt.com هستند درباره‌ی ویروس‌های کامپیوتری از من سوال می‌کنند: اینکه ویروسهای کامپیوتری چیستند؟ چگونه گسترش می‌یابند و چگونه کامپیوترها را آلوده می‌سازند و برای ما چه تهدیدی به شمار می‌آیند؟ دوستان از من می‌پرسند که چگونه می‌توانیم کامپیوترهایمان را از آلوده شدن به انواع و اقسام ویروسها محافظت و مراقبت کنیم. به لحاظ اهمیت موضوع، قصد داشتم تا در یکی از شماره‌های خبرنامه به زبانی ساده به ارائه تعریفی از ویروس‌های کامپیوتری و بررسی راه‌های مقابله با آنها بپردازم. از آنجا که مطلب برای گفتن بسیار بود و در طی زمان سوالات دیگری نیز از سوی اعضای خبرنامه‌هایم مطرح شد، تصمیم گرفتم که این مطالب را که به صورت یک جزوه الکترونیکی بر روی سایت و در اختیار همه اعضاء خبرنامه‌ها و نیز سایر بازدیدکنندگان از سایت قرار دهم. امیدوارم آنچه که در اینجا می‌آید بتواند گوشه ای از سوالات شما را پاسخ دهد. از شنیدن یا خواندن نظرات و پیشنهادهای سازنده‌ی شما بسیار خوشحال می‌شوم.

همانطور که انواع و اقسام ویروسها، به انسانها حمله می‌کنند و آنان را مبتلا می‌سازند، ویروس‌های کامپیوتری نیز می‌توانند به کامپیوترهایتان حمله کنند و آنان را آلوده کنند. ویروس‌های کامپیوتری برنامه‌ها و نرم افزارهایی هستند که اغلب خودشان را به برنامه‌ها و نرم‌افزارها و اسنادی که (از طریقی مثلاً از طریق دریافت فایل، دریافت نامه‌های الکترونیکی که فایلی به پیوست خود دارند) دریافت می‌کنید متصل می‌سازند. وقتی که برنامه‌ی ویروسی یا فایلی که به ویروس آلوده است را اجرا می‌کنید، ویروس می‌تواند نرم‌افزار کامپیوترتان را آلوده کند. ویروسها انواع و اقسام بسیاری دارند و به همین ترتیب اصطلاحات بسیاری برای نام بردن آنها در بین کاربران کامپیوترها متداول است. اما وقتی که اصطلاح کلی «ویروس» را به کار می‌بریم، بیشتر برای راحت‌تر شدن قضایا ست.

در مورد ویروسهای بیماری زا، ما (انسانها یا کلاً موجودات زنده) به نوعی «میزبان» هستیم. ویروسها برای آنکه رسالت خودشان را انجام دهند یا برای اینکه زنده یا باقی بمانند، نیاز دارند که از «میزبانی» به «میزبان دیگری» نقل مکان کنند. وقتی که سرما می‌خوریم، عطسه و سرفه می‌کنیم، اگر جلوی دهانمان را نگیریم، ذرات فوق‌العاده ریزی این ویروسها را در هوا منتشر می‌سازند و باعث می شوند که افراد دیگر نیز آلوده شوند و این آلودگی ویروسی به سرعت منتشر می‌شود. ویروسهای کامپیوتری هم برای اینکه باقی بمانند بگونه‌ای برنامه ریزی شده اند که خود را به سرعت منتشر کنند و اصطلاحاً از «میزبانی» به «میزبانی دیگر» نقل مکان می‌کنند.

آن ذرات ریزی را که در مورد ویروسهای بیماری زا گفتم، در مورد ویروسهای کامپیوتری، فایل‌ها، برنامه‌ها، نرم افزارها و گاه اسناد یا Document هایی هستند که نقش حمل کننده را برای ویروسها ایفا می‌کنند. ویروسهای کامپیوتری به گونه‌ای طراحی و برنامه ریزی شده‌اند که از کامپیوتر شما به کامپیوترهای دیگر وارد شوند و از آنجا نیز خود را به کامپیوترهای دیگری برسانند که به نوعی (مستقیم یا غیر مستقیم) با کامپیوتر اولی در ارتباط بوده‌اند، مثلاً شبکه های کامپیوتری محلی یا شبکه های گسترده تری چون اینترنت. بعضی از متداول ترین راههای منتشر شدن ویروسها را سعی می کنم در اینجا بیاورم.

۱ – وقتی سیستم شما به ویروسی آلوده می‌شود، ممکن است به صورت خودکار و خیلی سریع با استفاده از آدرس‌های پست الکترونیکی دوستان و آشنایانتان که در دفترچه آدرسها یا همان Address Book در برنامه پست الکترونیک‌تان وجود دارد، نامه‌های الکترونیکی حاوی نسخه‌هایی از «ویروس» را ارسال کند. به این نوع از ویروسها، «کرم» یا Worm گفته می‌شود چرا که خودش می‌تواند ویروس خودش را زیاد کند. اواخر ژانویه ۲۰۰۳ یک «کرم اینترنتی» براحتی توانست دهها هزار کامپیوتر را در سرتاسر این گرداب گسترده گیتی عملاً فلج کند و همان «کرم» باعث کند شدن بخشهایی از اینترنت شد.

۲- ویروسهای ماکرو (مثلاً نوعی که خودش را به اسناد Microsoft Word متصل می‌کند) نوعی دیگر از ویروسهای کامپیوتری به شمار می‌آیند. این نوع ویروس می‌تواند خودش را به هر نوع سندی که ایجاد می‌کنید یا تغییر می‌دهید بچسباند. وقتی شما سندی که آلوده شده است را با پست الکترونیک برای دوستتان ارسال کنید، براحتی عطسه ای کرده اید (: و ویروس را به کامپیوترش منتقل کرده اید.

۳- بعضی وقتها ویروسهای کامپیوتری به شکل و شمایل برنامه های تفریحی، بازی و سرگرمکننده (مثل کارت های تبریک الکترونیکی یا برنامه‌های محافظ صفحه‌ی نمایش) وارد سیستم شما می‌شوند و مخفیانه کامپیوترتان را آلوده می سازند. اگر این برنامه ها را دریافت کنید و متوجه ویروسی بودن آنها نباشید، ممکن است خودتان با دست خودتان آن برنامه‌ی ویروسی را برای دوستان و آشنایان و همکارانتان ارسال کنید.

۴- اسب‌های تروا Trojan Horses نوعی ویروسهای کامپیوتری به شمار می‌آیند، اما تفاوت‌هایی هم با آنها دارند و آن این است که این نوع ویروس‌ها سعی ندارند که خودشان زیاد یا تکثیر کنند. این برنامه‌ها از نوع «حمله کننده از درون» بوده، وارد سیستمها می‌شوند، ظاهراً شکل و شمایل و محتوایی بی آزار دارند اما اعمالی انجام می‌دهند که برای آن برنامه ریزی شده‌اند که مطلوب نظر یا به نوعی مفید برای ما نیست. مثلاً برنامه‌هایی که یک ورودی دروغین یا اصطلاحاً Fake Login را شبیه سازی می‌کنند تا اطلاعات اکانت، کد کاربری و رمز ورودی یا اطلاعات کارت اعتباری شما را بربایند.

بسیاری از ویروسهای کامپیوتری حقیقتاً نفرت انگیز و پلیدند چرا که می‌توانند فایلهای شما را بسرعت و به راحتی پاک کنند یا موجب قفل شدن کل سیستم یا شبکه‌ی شما شوند. غیر از این ویروسها، بقیه ویروسها مستقیماً کاری در جهت خرابی انجام نمی دهند و تقریباً بی آزارترند چرا که فقط با تکثیر خودشان، موجب کند شدن سیستمها به صورت محلی و یا کند شدن اینترنت یا اتصال به آن می‌شوند.
همانطور که در بالا نیز به آن اشاره کردم، ویروسها، برنامه ها و نرم افزارهایی هستند که با قصد و غرضی خاص نوشته شده اند، در حقیقت ویروسها می‌توانند باعث واردآوردن آسیب های جدی به سیستم های شما شوند. اینکه یک ویروس تا چه حد می‌تواند به سیستم (های) شما آسیب برساند به عوامل متعددی بستگی دارد از جمله اینکه تا چه حد استادانه نوشته شده باشد. بعضی از ویروسها می‌توانند فایلهای شما را کالاً پاک کنند یا تغییر بدهند، بعضی از ویروسها می‌توانند تمام اسناد یا Document های شما را پاک کنند یا حتی هارد دیسک تان را به آنی فرمت Format کنند و کامپیوترتان را از کار بیاندازند. بعضی از ویروسها می‌توانند اطلاعات محرمانه شما را مثلاً اطلاعات کارت‌های اعتباری، شماره های حسابهای بانکی، رمزهای ورودی Login Passwords را به صورت رندوم به آدرسهای پست الکترونیکی متعدد یا به آدرس پست الکترونیک ویروس نویس ارسال کنند. بعضی از ویروسها می توانند موجب کند شدن شدید سیستم شما شوند.

برخی دیگر می‌توانند برنامه‌هایی برای جاسوسی روی دستگاه‌تان نصب کنند یا برنامه‌هایی که تنظیمات امنیتی روی سیستمتان را تغییر می‌دهند، این نوع ویروسها، راههای نفوذ به سیستمهای شما را برای هکرها باز می‌کنند و آنها براحتی می‌توانند وارد شده و اطلاعات تان را به سرقت ببرند. «کرم» ها می‌توانند اثراتی شدید روی شبکه‌های کامپیوتری و به خصوص اینترنت بگذارند.

اگر از برنامه های ویروس‌یاب استفاده نکنید، ممکن است که هیچگاه متوجه حضور و فعالیت ویروس بر روی دستگاه کامپیوترتان نشوید چرا که بسیاری از ویروسها با تغییر نام دادن خودشان و یا متصل شدن به برنامه‌های اجرایی معمول و نصب شده روی کامپیوترتان به نوعی خودشان را پنهان می‌کنند. اما آلوده شدن کامپیوتر به ویروس، علایمی از خود بروز می‌دهد. ممکن است کامپیوترتان پیامهای عجیب و غریب نمایش دهد، ممکن است شروع به نواختن موسیقی کند یا برنامه هایی را پشت سر هم و بدون کنترل شما باز و بسته کند. ممکن است کامپیوترتان دیرتر بالا بیاید یا اصطلاحاً بوت شدن یا شروع برنامه های آن طولانی تر از روال معمول شود. ممکن است کامپیوتری که ویروسی شده، حافظه کم بیاورد یا فضای هارد دیسک به شدت کاهش یابد. بنابر این استفاده از برنامه‌های ویروس یاب معتبری چون نورتون و مک آفی برای اسکن کردن دوره‌ای کامپیوتر و حصول اطمینان از اینکه دستگاه بدون ویروس است را به شما توصیه می‌کنم.

تهیه برنامه‌های ویروس‌یاب، حفظ و نگهداری و به روزرسانی این

نرم‌افزارهای معتبر مسلماً هزینه ای را به شما تحمیل می کند که باید این هزینه ها را هم به عنوان بخشی از هزینه های مرتبط با خرید و نگهداری کامپیوتر(هایتان) در نظر بگیرید. تنها با استفاده از برنامه های ویروس یاب است که می توانید از وضعیت و سلامتی سیستم‌های خودتان مطمئن باشید. نصب برنامه‌ی ویروس یاب، اولین گام در حفظ و نگهداری سیستم شما است، اما این کافی نیست، لازم است تا برنامه ویروس یاب خود را هر از گاهی (طبق توصیه های شرکت تولید کننده ویروس یاب – که از طریق اینترنت یا فروشندگان به اطلاع‌تان می رسد – نسخه نصب شده را به روز رسانی یا اصطلاحاً Update کنید) . اگر ارتباط تان با اینترنت برقرار است می توانید برنامه ویروس‌یاب خود را به گونه‌ای تنظیم کنید که Update ها را – اطلاعات مربوط به کرمها یا ویروسهای جدید – به طور خودکار نصب کند و یا اینکه برنامه ویروس یاب در زمانهای معین پیام هایی جهت یادآوری نصب بر روی صفحه نمایش نشان دهد. به روزرسانی برنامه‌های ویروس یاب از اهمیت بالایی برخوردار است چرا که به طور تقریبی – بر اساس آمار منتشر شده – ماهی بیش از ۵۰۰ ویروس جدید کشف و شناسایی می‌شود. همانطور که گفتم، آنتی ویروس نورتون و ویروس اسکن مک آفی دو تا از بهترین و شناخته شده ترین برنامه های ویروس‌یاب معتبر برای سیستم عامل ویندوز می باشند. کاربر کامپیوترهای مک در ایران کم داریم، اما برای مکینتاشی ها هم آنتی ویروس نورتون و وایرکس مک آفی برای مکینتاش از این دو کمپانی بزرگ موجود است. لینوکسی ها هم می توانند از آنتی ویروس RAV استفاده کنند. اگر چه بیشتر ویروسها برای آلوده ساختن سیستم های مبتنی بر ویندوز نوشته شده اند اما کاربران کامپیوترهای مکینتاش و استفاده کنندگان از سیستم عامل لینوکس نیز باید با نصب ویروس یاب های معتبر از کامپیوترهایشان در مقابل ویروسها محافظت کنند. تقریباً همه‌ی ویروس یاب ها و برنامه‌های ضد ویروس موجود در بازار می‌توانند حافظه و دیسک سخت کامپیوترتان را در مقابل ورود و آلوده ساختن فایلها محافظت کنند، اما بسته های نرم افزاری با قابلیت ها و توانایی های مختلف می‌توانند نامه‌های الکترونیکی و فایل های آلوده و متصل به آنها را شناسایی کنند، ویروسهایی که از طریق برنامه های IM (پیام رسانی آنی = Instant Messaging مثل ICQ یا یاهو مسنجر) را شناسایی کنند، فایل های آلوده دریافت شده از طریق اینترنت (Downloaded Files) را پیش از باز کردن یا اجرا کردن شناسایی و پاک کنند. توجه داشته باشید که کامپیوتر شما تنها زمانی به ویروس آلوده می‌شود که شما فایل آلوده و ویروسی را (مثل فایل های زیپ شده) باز کنید، مشاهده کنید (اسناد) یا اینکه آن را اجرا کنید (در مورد فایل هایی که اجرایی هستند) - بنابر این توصیه من به شما این است که فایل های جدیدی که از اینترنت دریافت یا Download می کنید را پیش از باز کردن یا اجرا کردن، بوسیله آنتی ویروس خود اسکن کنید. حتی الامکان برنامه ها و نرم‌افزارهای کاربردی و لازم خود را از سایتها و شرکت های نرمافزاری شناخته شده و معتبری چون :

http://www.download.com
http://www.tucows.com
http://downloads-zdnet.com.com

که برای دریافت یا Download فایل و نرم‌افزار بگیرید. ابتدا نرم افزار مورد نظر خود را دریافت و بر روی هارد ذخیره کنید و بعد بلافاصله پس از اتمام دریافت فایل آن (ها) را توسط برنامه ویروس یاب یا آنتی ویروس خود اسکن کنید. برنامه آنتی ویروس خود را به گونه ای تنظیم کنید که نامه‌های ارسالی و دریافتی شما را پیش از ارسال و یا دریافت اسکن کند. این ممکن است که سیستم شما کمی کند اما از من بشنوید که این به نفع شماست. بسیاری از ویروسهای کامپیوتری از طریق فایلهایی که به نامه‌های الکترونیکی متصل اند به کامپیوترها راه می یابند بابر این دور از انتظار نیست که بسیاری از کارشناسان امنیت سیستم ها به مردم توصیه می‌کنند که در برنامه های ایمیل خود، (برنامه هایی مثل Microsoft Outlook یا Outlook Express و یا Eudora) دریافت نامه ها را به گونه ای تنظیم کنند که مانع از دریافت فایلهای پیوست شده به نامه‌های الکترونیکی شود، ارزشش را دارد خصوصاً به هنگام دریافت نامه از افراد ناشناس.

به طور متوسط، روزانه ۶ تا ۸ ویروس جدید شناخته می‌شود و ویروس‌ها به قولی آمده‌اند که بمانند. هم اکنون صحبت از ویروسهایی برای تلفن‌های همراه هم به میان آمده است. گرداب گسترده گیتی با تمام حسن هایش، به نوعی تهدیدهایی را هم برای شما و ما به همراه دارد که باید خودمان را در مقابل این تهدیدها همواره آماده و هوشیار نگاه داریم. آیا باید از ویروسها بترسیم؟ به نظر من، ترس از ویروسها، بی مورد است چرا که آنتی ویروسها، که توسط شرکتهای بزرگ و معتبر بین‌المللی عرضه می‌شوند و به سرعت خودشان را Update می‌کنند و در شرایطی که ما برنامه‌های آنتی ویروس نصب شده روی کامپیوترهایمان را به موقع به روز رسانی کنیم، می‌توانند به کمک ما بیایند. با استفاده از آنها به سرعت میتوانیم پیش از اینکه کامپیوترهایمان آلوده شود، آنها را شناسایی کنیم و از بین ببریم. برخی از دوستان می‌پرسند که آیا فایل‌های اطلاعاتی (Data Files) هم ممکن است به ویروس آلوده شوند؟ پاسخ این سوال این است که «معمولاً نه. فقط یک استثناء وجود دارد و آن هم در مورد دیتا فایلهایی است که حاوی کدهای اجرایی هستند، این فایلها ممکن است به ویروس آلوده شوند. برای یک مثال خوب در این مورد می توان فایلها و اسناد Microsoft Word (فایلهای DOC. و DOT.) را نام برد. اگرچه فایلهای word اساساً جزو دیتا فایلها به حساب می‌ایند، اما ممکن است حاوی ماکروهایی باشند که اجرایی هستند و بنابر این انتظار این می‌رود که به ویروس هم آلوده شوند. امروزه بیشتر موارد ویروسی که گزارش شده اند جزو این دسته از ویروسهای ماکرو می‌باشند.

با ارسال این فایل PDF برای دوستان خود، خواندن این مقاله را به آنان توصیه کنید. با بازدید از سایت www.webfaqt.com مقالات رایگان دیگری را به قلم تابان خواجه‌نصیری (در صفحه مقالات و در بخش فارسی سایت) در زمینه‌های مرتبط با بازاریابی اینترنتی و فن‌آوری اطلاعات بیابید و بخوانید.

برای عضویت در خبرنامه‌های رایگان تابان خواجه‌نصیری در سایت WEBFAQT.COM می‌توانید یکی از فرمهای تماس در سایت را پر نموده و به نامه‌ای که برایتان ارسال می‌شود پاسخ بدهید.

آماده پذیرش آگهی های شما در این فایل هستیم – با ما تماس بگیرید!