طرز کار برنامه هاي ضد ويروس

ضد ویروس اصطلاحی است که به برنامه یا مجموعه ای از برنامه ها اطلاق می شود که برای محافظت از کامپیوتر ها در برابر ویروس ها استفاده می شوند .مهم ترین قسمت هر برنامه ضد ویروس موتور اسکن
(Scanning engine)آن است .جزئیات عملکرد هر موتور متفاوت است ولی همه آنها وظیفه اصلی شناسایی فایل های آلوده به ویروس را با استفاده از فایل امضای ویروس ها بر عهده دارند. فایل امضای ویروس یک رشته بایت است که با استفاده از آن می توان ویروس را به صورت یکتا مورد شناسایی قرار داد و از این جهت مشابه اثر انگشت انسان ها می باشد. ضد ویروس متن فایل های موجود در کامپیوتر را با نشانه های ویروس های شناخته شده مقایسه می نماید. در بیشتر موارد در صورتی که فایل آلوده باشد برنامه ضدویروس قادر به پاکسازی آن و از بین بردن ویروس است. در مواردی که این عمل ممکن نیست مکانیزمی برای قرنطینه کردن فایل آلوده وجود دارد و حتی می توان تنظیمات ضدویروس ها را به گونه ای انجام داد که فایل آلوده حذف شود.

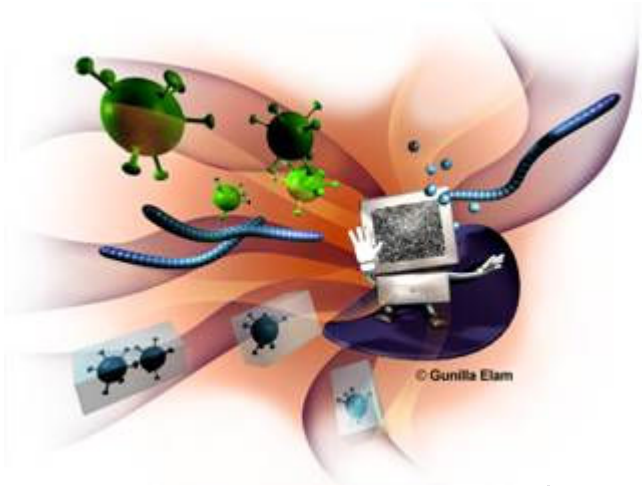
بعضی از برنامه های ضد ویروس برای شناسایی ویروس های جدیدی که هنوز فایل امضای آنها ارائه نشده از روش های جستجوی ابتکاری استفاده می کنند .به این ترتیب داده های مشکوک در فایل های موجود در سیستم و یا فعالیت های مشکوک مشابه رفتار ویروس ها (حتی در صورتی که تعریف ویروسی منطبق با آنچه که در فایل مشکوک یافت شده موجود نباشد (علامت گذاری می شوند. اگر ضد ویروس فعالیت مشکوکی را مشاهده نماید، برنامه ای که فعالیت مشکوک انجام داده را قرنطینه نموده و به کاربر در مورد آن اعلام خطر می کند) به عنوان مثال اعلام می شود که برنامه مشکوک مایل به تغییر Windows Registry می باشد). دقت این روش پایین است و در بسیاری از مواقع در شناخت فایل های مشکوک به ویروس اشتباهاتی رخ می دهد.

در چنین مواقعی فایل قرنطینه شده برای شرکت های سازنده ضد ویروس ها ارسال می شود که پس از تحقیق و آزمایش آن، در صورتی که واقعا فایل آلوده به ویروس باشد نام، امضاء و مشخصات آن مشخص شده و پادزهر آن ارائه می گردد .در این صورت کد مشکوک تبدیل به یک ویروس شناخته شده می شود.

قابلیت های نرم افزار های ضدویروس

سطح محافظت نرم افزار بسته به جدید و بروز بودن آن متغیر است .محصولات جدیدتر قابلیت های مانند بروز رسانی خودکار، اسکن های زمان بندی شده، محافظت از سیستم به صورت ماندگار در حافظه و همچنین امکان یکپارچه شدن با برنامه های کاربردی اینترنتی مانند برنامه های e-mail و مرورگرهای وب را دارند. نسخه های قدیمی تر نرم افزارهای ضدویروس تنها یک اسکنر بودند که باید به صورت دستی راه اندازی می شدند. همه نرم افزار های ضدویروس در صورتی که به صورت منظم به روز رسانی شده و عملیات اسکن بر روی دیسک های سخت، تجهیزات قابل انتقال (مانند فلاپی و Zip disk) انجام شود می توانند دستگاه کامپیوتر را در برابر ویروس ها مقاوم کنند. در واقع نقطه برتری محصولات جدید ضد ویروس در قابلیت های آنها برای محافظت از سیستم در مواقعی است که کاربر دانش و یا دقت لازم برای به کارگیری آن را ندارد.

حداقل توقعی که از یک برنامه ضد ویروس خوب می توان داشت این است که در برابر ویروس های boot-sector، ماکرو، اسب های تروا و فایل های اجرایی آلوده به ویروس و کرم اقدامات محافظتی لازم را به عمل آورد. از محصولات جدیدتر می توان انتظار محافظت در برابر صفحات وب، اسکریپت ها، کنترل های ActiveX و اپلت های جاوای خطرناک، همچنین کرم های e-mail را داشت.



قابلیت‌هاي نرم‌افزارهاي ضدويروس

در قسمت‌های قبلی از این مجموعه مقالات ضمن معرفی انواع ویروس‌ها و سایر برنامه‌های مختل کننده امنیت، چگونگی کشف ویروس‌ها توسط برنامه‌های ضدویروس و تعدادی از قابلیت‌های برنامه‌های ضدویروس بیان شد. در این مقاله چند قابلیت مهم نرم‌افزارهای ضدویروس مورد بررسی قرار می‌گیرد.

تفاوت بین نسخه‌های ضد ویروس

همه نرم‌افزارهای ضد ویروس عمل واحدی را انجام می‌دهند که همان اسکن فایل‌ها و پاک‌سازی موارد آلوده می‌باشد. بعضی از آنها حتی از موتورهای اسکن یکسانی برای شناسایی ویروس‌ها بهره می‌گیرند. تفاوت اصلی بین این محصولات در کیفیت واسط کاربر، سرعت و دقت محصول و قابلیت‌های خاص (مانند اسکنرهایe-mail ، بروز رسانی‌های خودکار زمان بندی شده، اسکن‌های ابتکاری و ...) می‌باشد .

در حال حاضر با توجه به اتصال اکثر کامپیوترها به شبکه اینترنت و خطرات گسترده‌ای که از این طریق کاربران را تهدید می‌کند تامین امنیت در برابر ویروس‌هایی که از طریق اینترنت انتقال می‌یابند اهمیت زیادی دارد. از سوی دیگر اینترنت می‌تواند به عنوان ابزاری برای بروز نگه‌داری نرم‌افزارهای ضدویروس مورد استفاده قرار گیرد.

حافظت e-mail

افزایش تعداد کرم‌هایی که از طریق e-mail توزیع می‌شوند نیاز همه افراد به محصولات ضد ویروسی که امنیت آنها را تامین کنند افزایش داده است .تعدادی از محصولات نرم‌افزاری نمی‌توانند امنیت مورد نیاز را برای همه کاربران تامین کنند. از سوی دیگر تمایل زیاد کاربران به یکپارچه سازی نرم افزارهای

e-mail با برنامه‌های اداری باعث شده، شکاف‌های امنیتی موجود در نرم‌افزارهای اداری توسط کرم‌هایی مانند ILOVEYOU و W32.Klez به سادگی مورد استفاده قرار گیرد. در چنین مواردی اگر وصله‌های امنیتی سیستم قدیمی باشند(که این مساله بسیار رایج است)، تنها مشاهده یک نامه آلوده کافی است که کرم به دستگاه نفوذ کند.

مشکل اصلی در رابطه با امنیت e-mail به نحوه کار برنامه‌ها برمی‌گردد. برنامه‌های e-mail پیام‌ها را دریافت کرده و آنها را در پایگاه‌داده‌های خاص خود ذخیره می‌نمایند. از سوی دیگر برنامه‌های ضد ویروس فقط فایل‌هایی را که در قالب فایل‌سیستم‌های شناخته شده مانندFat16، Fat32 ، NTFS و ... هستند را اسکن می‌کنند، بنابراین لزوما نمی‌توانند ساختمان داده‌ای را که برنامه e-mail برای ذخیره سازی اطلاعات استفاده می‌کند شناخته و پیام‌های ذخیره شده و فایل‌های ضمیمه آن را اسکن کند. این بدان معناست که هرگاه یک e-mail آلوده بر روی دستگاهی که وصله‌های جدید بر روی آن نصب نشده بار شود، نه تنها کامپیوتر آلوده می‌شود بلکه پاک کردن دستگاه به سادگی امکان پذیر نیست و حتی ممکن است همهe-mail ها از دست بروند. به عنوان مثال کرم W32.Klez که کامپیوترهای زیادی را آلوده نمود، در گام اول برنامه‌های ضد ویروس را مورد هجوم قرار می‌دهد و در نتیجه برنامه آلوده شده قادر به پاک کردن محتویات صندوق‌های پستی کاربران نیست.

دو راه حل برای این مشکل وجود دارد، یا باید با دقت همه وصله های جدید مرورگر وب و برنامه‌های

e-mail را گرفته و بر روی دستگاه نصب نمود و یا از برنامه‌های ضدویروسی استفاده کرد که به مرورگر و برنامه mail متصل شده و آنها را به روز نگه‌می‌دارند.

برای اینکه سیستم e-mail کاملا حافظت شده باشد، باید عملیات اسکن قبل از اینکه e-mail در جایی از حافظه ذخیره شود صورت گیرد. به عبارت دیگر برنامه e-mail داده را بعد از گرفتن از اینترنت به اسکنر ضدویروس ارسال می‌نماید تا عملیات لازم بر روی آن صورت گیرد.

همه نرم‌افزارهای e-mail قابلیت این نوع مجتمع شدن را ندارند. اما اسکنرهایی وجود دارند که به خوبی با بعضی از نسخه‌هایMicrosoft Outlook Express، Microsoft Outlook ، Netscape Messenger،Netscape Pro ، Eudora و Becky Internet Mail مجتمع می‌شوند. بعضی از اسکنرها ادعای مجتمع شدن با همه سرویس‌گیرنده‌های POP3 و MAPI را مطرح می‌کنند.

بروز رسانی نرم‌افزارهای ضدویروس

نصب برنامه ضد ویروس و رها کردن آن برای داشتن دستگاهی بدون ویروس و مقاوم در برابر حملات ویروس‌ها کافی نیست. هر روزه ویروس‌های جدیدی عرضه می‌شود و در سال‌های جدید انتشار سریع کرم‌ها از طریق اینترنت نرخ ایجاد ویروس را افزایش داده است. این مساله در ترکیب با افزایش دانش عمومی در مورد مشکلات امنیتی نرم‌افزارها و سیستم‌های عامل سرعت ایجاد ویروس‌های جدید را افزایش داده است .امروزه برای ایجاد یک ویروس نیاز به مهارت و تخصص زیاد نیست. تولید کنندگان ویروس‌ها می توانند ویروس‌هایی با تفاوت‌های اندک نوشته و در دنیای مجازی انتشار دهند. بنابراین علاوه بر خرید و نصب نرم‌افزار ضدویروس دقت در بروز نگه‌داشتن آن هم از اهمیت خارق‌العاده‌ای برخوردار است.

شرکت‌های تولید کننده نرم‌افزار برای مقابله با این مشکل قابلیت بروز رسانی خودکار را به محصولات جدید خود افزوده‌اند. بنابراین کاربران تنها با انتخاب گزینه مناسب از منوهای نرم‌افزار می‌توانند از بروز بودن نرم‌افزار خود مطمئن باشند .

سربلند باشید

منبع :

امین بدیعي
webmaster@isfahan4u.com