به نام خدا

وزارت ارتباطات و فناوری اطلاعات

اداره کل ارتباطات و فناوری اطلاعات استان اصفهان

کرم های کامپیوتری

مرداد ماه ۹۲

مقدمه:

آیا تا به حال اتفاق افتاده که وقتی شما هیچ کاری با سیستم کامپیوتری خود انجام نمی‌دهید، شاهد باشید که سیستم تحت بار کار قرار دارد و برنامه‌هایتان به کندی اجرا می‌شوند؟ یا زمانی که به اینترنت وصل هستید و از جانب شما هیچگونه تبادل اطلاعاتی انجام نمی‌شود، چراغهای گرفتن و فرستادن اطلاعات کماکان روشن هستند و برقراری ارتباط با اینترنت کندتر و کندتر می‌شود؟

اولین کرم کامپیوتری در آمریکا در روز سوم نوامبر ۱۹۸۸ کشف شد. در آن روز بسیاری از سیستمهای کامپیوتری عملاً توانایی انجام عملیات را از دست دادند.

یک کرم کامپیوتری چیست و چه تفاوتی با ویروسهای کامپیوتری دارد؟ویروسهای کامپیوتری برنامه‌های مخربی هستند که برای انتقال از یک سیستم کامپیوتری به سیستم دیگر باید حتماً خود را به یک فایل اضافه کنند. بدین ترتیب امکان انتقال ویروسها تنها از طریق دریافت و اجرای فایل‌های آلوده به شکل نامه‌های الکترونیکی و یا فایل‌های اجرایی و مشابه آنها امکان‌پذیر است. همچنین ویروس‌ها خودشان را داخل یک سیستم تکثیر می‌کنند و تا زمانی که شما به عنوان کاربر کامپیوتر دخالتی نداشته باشید، هیچ ویروسی به سیستم دیگر منتقل نخواهد شد. مشکل زمانی پیش می‌آید که شما کار کپی فایل‌های آلوده را انجام می‌دهید و فایل‌ها به همراه ویروس موجود در آنها به سیستم دیگری منتقل می شوند، درحالی که کرم‌ها روش دیگری برای انتقال خود دارند.

وقتی شما به اینترنت یا هر شبکه کامپیوتری دیگری وصل می‌شوید، با بسیاری از سیستمهای کامپیوتری دیگر در ارتباط هستید. کرمها طوری طراحی می‌شوند که خود به خود از مسیرهای ارتباطی کامپیوترها با یکدیگر عبور کرده و به سیستمهای دیگر نفوذ می‌کنند. بدین ترتیب نقش کاربر در انتقال کرم‌ها در حداقل خود قرار دارد. کرمها خودشان را به فایل‌ها نمی‌چسبانند، اما زمانی که به هر شکل تبادل اطلاعات بین سیستم‌های کامپیوتری انجام می‌شود، کرم‌ها مسیر را دنبال کرده و به سیستم مقصد وارد می‌شوند. بدین ترتیب هر شکلی از فعالیت ارتباطی بین سیستم‌های کامپیوتری را از جمله دریافت ایمیل حتی بدون خواندن آن، چت کردن به شکل متنی، صوتی و تصویری و نیز ارسال و دریافت فایلهای مختلف حتی بسیار کوتاه و مختصر می‌تواند راه را برای نفوذ کرم‌ها به سیستم شما باز کند. بخصوص سایت‌هایی که به طور اتوماتیک پیشنهاد دانلود کردن برنامه‌های خاص را می‌دهند، در این مورد بسیار راه نفوذ خطرناکی هستند. بنابراین درحالی که ویروس‌ها فقط از طریق بعضی فایل‌های خاص منتقل می شوند، در مورد کرم‌ها هیچ محدودیتی وجود ندارد. ضمناً یکی از بزرگترین

معضلات کرم‌ها این است که به افراد ثالث این امکان را می‌دهد که بدون اجازه شما از طریق اینترنت به سیستم کامپیوتری شما دسترسی پیدا کنند و آنچه دلشان می‌خواهد انجام دهند.

به علاوه، ویروس‌ها برای انجام یک کار مشخص مثلاً خراب کردن سکتور صفر هارد دیسک و یا آلوده کردن فایل‌های اجرایی برای جلوگیری از انجام آنها طراحی می‌شوند و در کل هر ویروس وظیفه مشخصی به عهده دارد. اما کرم‌ها کار مشخصی انجام نمی‌دهند. تنها کاری که کرم‌ها می‌کنند، این است که تمام منابع سیستم شما را اشغال می‌کنند. در حافظه جایگزین می‌شوند، بار کار پردازنده مرکزی را افزایش می‌دهند، اطلاعات فزاینده‌ای زمان ارتباط با اینترنت دریافت و ارسال می‌کنند و بدین ترتیب عملکرد سیستمی که تمام منابعش توسط کرم‌ها اشغال شده، آنقدر پایین می‌آید که عملاً از کار می افتد. وقتی یک کرم وارد سیستم شما می‌شود، معمولاً اطلاعی از ورود خودش نمی‌دهد و کار را به صورت پنهانی آغاز می‌کند. کرم‌ها علاوه بر ارسال خودشان به سیستم‌های دیگر، در سیستم اولیه نیز به تعداد انبوه تکثیر می‌شوند. در بهترین حالت ویروس بعد از اینکه کل سیستم شما را در اختیار گرفت، حضورش را به شکل یک متن یا تصویر یا آهنگ اعلام می کند، اما در طول زمانی که کرم در سیستم شما وجود دارد، هیچ اعلام مشخصی از آن صورت نمی‌گیرد. مطمئن‌ترین راه برای جلوگیری از ورود کرم‌ها به سیستم شما، نصب کردن برنامه‌های ضد ویروس جدید است که کرم‌ها را نیز شناسایی می کنند. البته این کار خود به خود عملکرد سیستم را به شدت تحت تأثیر قرار می‌دهد، اما به نظر می‌رسد در شرایط موجود، تنها گزینه ممکن برای جلوگیری از کرم، گذشتن سیستم شما است!

ذکر چند نمونه از نفوذگرها در اینترنت:

:Spywaer

هر برنامه‌ای که به صورت مخفیانه و بدون آگاهی کاربر به کامپیوتر وارد شود Spy نامیده می شود. Spy waerها می‌توانند فعلیت‌های تخریبی بی‌شماری انجام دهند. مثلا می‌توانند شماره کارت‌های اعتباری و یا آدرس‌های ایمیل و همچنین پسوردها و غیره را استخراج کنند و تمامی اطلاعات را برای شخص نفوذگر بفرستند.

کرم اینترنتی یا Worm :

Worm: گونه‌ای از برنامه‌های تخریبی کرم اینترنتی یا Worm هستند و کار اصلی آنها تخریب اطلاعات شخصی بر اساس یک الگوی خاص و مشخص می‌باشد. این گونه برنامه‌ها بدون این که ردپایی از خود باقی بگذارد اطلاعات را تخریب می‌کنند و در عین حال از کامپیوتری به کامپیوتر دیگر می‌روند. بعضی از این گونه کرم‌های اینترنتی بسیار بدتر از ویروس‌ها عمل می‌کنند چون از همه موانع امنیتی به راحتی عبور می‌کنند و اعمال تخریبی خود را انجام می‌دهند.

اسب تروآ یا Trojan:

Trojan: گونه دیگری از برنامه‌های تخریبی اسب تروآ یا تروجان Trojan می‌باشند. این گونه از برنامه‌ها در ظاهر وانمود می‌کنند که خوب و بی‌ضرر هستند اما در حقیقت هدف این گونه از برنامه‌ها خراب کردن و دزدیدن اطلاعات می‌باشند.

اسب‌های تروآ می‌توانند در زمان اتصال به اینترنت و یا از طریق ایمیل به سیستم وارد شوند و می‌توانند فایل‌ها را حذف و اضافه و یا تغییر دهند.

سیستم مانیتور:

System Monitor: سیستم مانیتور برنامه‌هاییبا کارایی متفاوت برای کنترل فعالیت‌های کاربران می‌باشند. این گونه از برنامه‌ها می‌توانند تمامی اطلاعات را از قبیل آدرس‌های Email، پسوردها، سایت‌های بازدید شده و کلمات تایپ شده توسط صفحه کلید را جمع‌آوری کنند. این گونه از برنامه‌ها حتی می‌توانند از فعالیت‌های کاربران عکس‌برداری کرده و عکس‌ها را بعلاوه سایر اطلاعات جمع‌آوری شده به آدرس ایمیلی خاص هدایت کنند.

BACK DOOR : گونه‌ای از برنامه‌ها که فرد نفوذگر به جا گذاشته و امکان نفوذ مجدد را برای دستیابی بعدی فراهم می‌کند.

TRACE : این برنامه نمونه‌ای از دسته برنامه‌های جاسوسی می‌باشد. این گونه از برنامه‌ها می‌توانند به صورت‌های مختلف سیستم را تخریب کنند. یعنی این برنامه‌ها می‌توانند به محیط ریجستری وارد شده و یا در حافظه رم مقیم شوند ویا به درون دیسکها منتقل شوند و حتی خود را به فایل‌ها بچسبانند و کار تخریبی انجام دهند. علاوه بر این گروه از ابزارهای تخریبی و جاسوسی گونه‌های دیگری ازاین قبیل ابزارها وجود دارند که سیستم را مورد هجوم و تخریب می‌دهند می‌توان از این گروه به ماکروها و EXPLOITها نیز اشاره کرد.

نرم‌افزارهای جاسوسی چگونه شما را کنترل می‌کنند؟

نرم افزارهای جاسوسی در اینترنت جزو خطرناک‌ترین نرم افزارها در جهان مجازی محسوب می‌شوند. این نرم افزارها می‌توانند با کنترل و مانیتور کردن فعالیت‌های افراد روی شبکه اطلاعات مهمی از سیستم‌های مورد استفاده به دست بیاورند. حتی در بی‌ضررترین حالت، Spyware تجاوز به حریم شخصی افراد است. نرم‌افزارهای Spyware (مانند Cydoor، Gator، Lop.com و Xupiter) بدون اطلاع کاربر و از طریق برنامه‌های به اشتراک‌گذاری فایل (peer-to-peer)،

نرم‌افزارهای مجانی و یا برنامه‌هایی که تصاویر زیبای مختلف را بر روی کامپیوتر نمایش می‌دهند، خود را بر روی کامپیوتر کاربران نصب می‌نمایند.

این‌گونه نرم‌افزارها که عمدتاً از آنها برای مقاصد تبلیغاتی هدفمند استفاده می‌شود، عادات وب‌گردی یک کاربر را ردیابی می‌کنند. برخی از آنها کلمات تایپ شده توسط کاربر و یا تصویر نمایش داده شده روی مانیتور را ثبت و برای صاحبان خود ارسال می‌کنند.

اجتناب از این برنامه‌ها بسیار مشکل است. زیرا اغلب به همراه افزونه‌های می‌آیند و بدون اینکه مشخص باشد خود را بر روی کامپیوتر نصب می‌کنند. در این حالت حذف کردن آنها بسیار سخت، زمان‌بر و هزینه‌بر می‌باشد.

در بدترین حالت این نرم‌افزارها اگر در دست افراد سودجو قرارگیرد، به ابزاری خطرناک تبدیل می‌شود. در این صورت می‌توان از آنها برای مقاصدی چون دستیابی به رمز عبور (password) افراد، سرقت شماره کارت اعتباری و سرقت سایر مدارک هویتی افراد استفاده کرد. حتی برخی از صاحب نظران مسائل امنیت کامپیوتری بر این باورند که از اینگونه نرم‌افزارها می‌توان برای اهداف خطرناکتری استفاده کرد: مثل ضبط‌کردن و انتقال دادن اسناد تایپ شده درMicrosoft Word و Microsoft Excel با هدف سرقت اطلاعات محرمانه شرکت‌ها.

چگونه جلوی Spyware را بگیریم؟

اولین خط دفاعی اجراکردن سیاست‌های استفاده از اینترنت در سطح شرکت می‌باشد:

- پیکربندی مرورگرهای اینترنت و نرم افزار Outlook با استفاده از Microsoft Domain Security،
- بستن ActiveX و سایر برنامه‌های قابل اجرا در اینترنت،
- مدیریت Script ها،
- پالایش‌کردن محتویات وب از طریق HTTP proxy،
- در صورت لزوم، عدم دسترسی پرسنلی که در انجام کارشان نیازی به اینترنت ندارند.

همچنین باید به پرسنل آموزش داده شود که چگونه از اینترنت به شکل بی‌خطر استفاده نمایند:

- برنامه‌های peer-to-peer یا هر برنامه‌ای که به آن اطمینان ندارند را نصب ننمایند،
- برروی تصاویر سرگرم کننده مثل خرس رقاص (Dancing Bear) کلیک نکنند،
- نرم‌افزارهای مجانی را بدون تأیید واحد IT سازمان نصب ننمایند.

چگونه Spyware ها را شناسایی کنیم؟

یکی از بهترین روش‌ها برای شناسایی Spywareها استفاده از نرم‌افزارهای پالایش محتویات وب، می‌باشد. شرکت Websense1 برروی محصول جدید خود، Client Application Module، منوی تازه‌ای بنام Spyware تعبیه کرده است. این شرکت با به‌روزآوری‌های روزانه بیشتر نرم‌افزارهای Spyware را قبل از ورود به شبکه شناسایی و به آنها اجازه راهیابی به کامپیوترهای شبکه را نمی‌دهد.

اگر برنامه‌ای از این فیلتر عبور کند، CAM اجازه اجرا و فعالیت را به آن نمی‌دهد. همچنین از طریق گزارشات Websense می‌توان پی‌برد که Spyware بر روی کدام یک از کامپیوترهای شبکه نصب شده است و برای پاک کردن آن اقدام نمود. نرم‌افزارهای ضدویروس مانند Eset Smart Security بعضی از آنها را شناسایی می‌کنند.

چگونه Spyware ها را از بین ببریم؟

از بین بردن Spywareهایی که از فیلتر رد می‌شوند، بدون استفاده از ابزارهای حذف اتوماتیک آنها، کاری بسیار مشکل می‌باشد. زیرا اغلب آنها به‌گونه‌ای طراحی شده‌اند که در مقابل uninstall مقاومت می‌کنند.

برخی شرکت‌های نرم‌افزاری اقدام به تولید برنامه‌های تشخیص‌دهنده و از بین برنده Spyware نموده‌اند. به عنوان مثال می‌توان به Ad-Aware محصول شرکت Lavasoft2 که نسخه معمولی آن مجانی می‌باشد و نرم افزار Spybot3 که آن هم مجانی می‌باشد اشاره کرد.

نرم‌افزار اخیر ظاهراً توانمندتر از نسخه معمولی Ad-Aware می‌باشد. البته شرکت‌هایی که از نرم‌افزاهایی مثل Websense استفاده می‌کنند اغلب نیازی به نرم‌افزارهای فوق ندارند مگر در موارد خاصی که کسی دچار مشکل می‌شود. از دیگر نرم‌افزارها در این زمینه می‌توان به موارد زیر اشاره کرد:

SpySubtract محصول شرکت InterMute4، نرم افزار LLC Mechanic محصول شرکت Iolo Technologies5، برنامه SSE firewalls محصول Sygate6 و در نهایت برنامه GhostSurf Pro محصول Tenebril7.

منابع:

http://www.iran-newspaper.com/

http://www.mirsoft.net

http://www.todayifoundout.com/index.php