پیام چادرملو

شماره دهم

بهار ۱۳۸۵

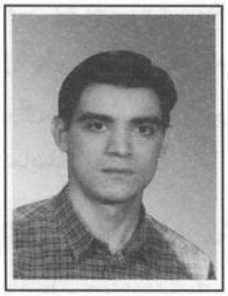
امنیت اطلاعات (قسمت اول: برنامه های مخرب)

مولف: مهدی ریزوندی

http://mrizvandi.com
info@mRizvandi.com
mRizvandi@yahoo.com

امنیت اطلاعات

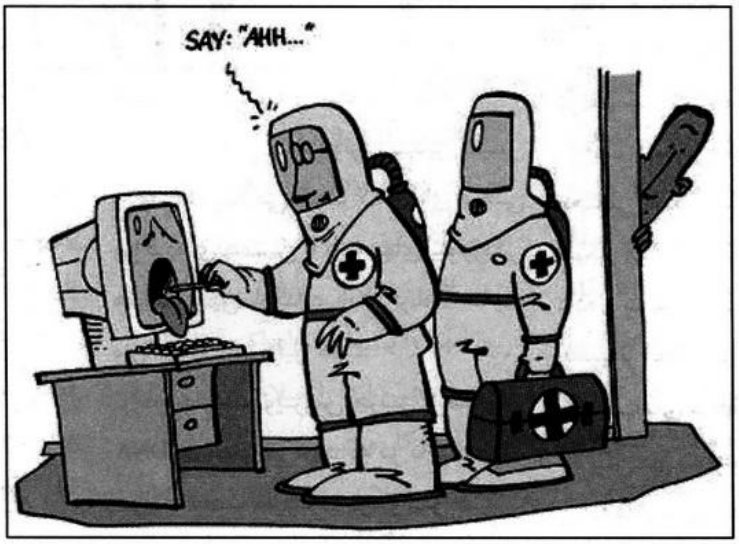
قسمت اول: برنامه‌های مخرب



تهیه شده در مرکز اطلاعات مدیریت و تعالی سازمانی
توسط: مهندس مهدی ریزوندی

مقدمه

امروزه در عصر ارتباطات و اطلاعات، امنیت مقوله‌ای بسیار بزرگ و دغدغه‌ای برای مدیران اطلاعات می‌باشد. چراکه شاهد گسترش حضور کامپیوتر در تمامی ابعاد زندگی خود می باشیم. کافی است به اطراف خود نگاهی داشته باشیم تا به اهمیت موضوع بیشتر واقف شویم. در جهت رسیدن به امنیت باید آگاهی لازم نسبت به این امر را داشت. همیشه مدیران اطلاعات در جهت فراهم آوردن امنیت اطلاعات گام برمی‌دارند ولی آیا رسیدن به یک نقطه امنیتی نشانگر امنیت است؟ مسلماً خیر. چرا که امنیت اطلاعات یک امر کاملا نسبی و رو به رشد است و هیچ گاه متوقف نخواهد شد. کاربران کامپیوتر به منظور استفاده از دستاوردها و مزایای فناوری اطلاعات و ارتباطات، ملزم به رعایت اصولی خاص و اهتمام جدی به تمامی مولفه‌های تاثیر گذار در تداوم ارائه خدمات در یک سیستم کامپیوتری می باشند. امنیت اطلاعات و ایمن سازی شبکه‌های کامپیوتری از جمله این مولفه‌ها بوده که نمی توان آن را مختص یک فرد و یا سازمان در نظر گرفت. در این خصوص کاربران سیستمهای کامپیوتری صرفنظر از مسئولیت شغلی باید به مقوله امنیت



اطلاعات نگاه ویژه داشته باشند.

تمامی کامپیوترها اعم از کامپیوترهای موجود در شرکت‌ها و منازل، در معرض آسیب و تهدیدات امنیتی می باشند .با انجام تدابیر لازم و استفاده از برخی روشهای ساده می توان پیشگیری لازم و اولیه‌ای را در خصوص ایمن سازی محیط کامپیوتری خود انجام داد. در این مقاله و قسمتهای بعدی سعی بر آن خواهد شد که آگاهی اولیه و نسبی در خصوص برنامه‌های مخرب، حفاظت از اطلاعات و سخت‌افزار و فرهنگ امنیت اطلاعات در جهت برقراری امنیت نسبی ارائه شود.

داده‌ها و اطلاعات حساس در معرض تهدید

تقریباً هر نوع تهاجم، تهدیدی است در مقابل حریم خصوصی، پیوستگی، اعتبار و صحت داده‌ها. یک سارق اتومبیل می‌تواند در هر لحظه صرفا یک اتومبیل را سرقت نماید، در صورتی که یک مهاجم با به کار گیری صرفا یک دستگاه کامپیوتر، می تواند آسیب‌های فراوانی را متوجه تعداد زیادی از شبکه‌های کامپیوتری نموده و باعث بروز اشکالاتی متعدد در زیر ساخت اطلاعاتی یک کشور گردد. آگاهی لازم در رابطه با تهدیدات امنیتی و نحوه حفاظت خود در مقابل آنان، امکان حفاظت اطلاعات و داده‌های حساس را در یک شبکه کامپیوتری فراهم می نماید.

به چند دلیل مدیران به فکر توسعه ایجاد امنیت اطلاعات هستند چراکه موارد بسیار زیادی در جهت تضعیف و سوءاستفاده از اطلاعات وجود دارد که از جمله می‌توان به برنامه‌های مخرب و برنامه‌های جاسوسی اشاره کرد. هر کدام از

این دو دسته مشکلات، ضرر و زیانهایی را برای یک شرکت و حتی برای یک شخص می تواند وارد نمایند.

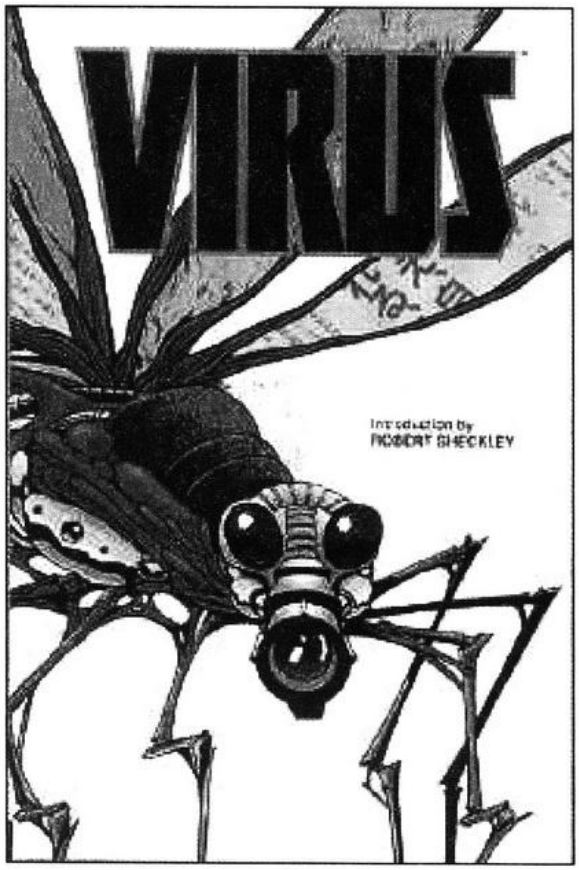
الف) برنامه‌های مخرب

کلیه برنامه‌هایی که می‌توانند اطلاعات را غیر قابل استفاده نمایند، جزو دسته برنامه‌های مخرب هستند. در بسیاری از موارد این تخریب در برنامه‌های اجرایی صورت می‌گیرد اما دسته‌ای از این برنامه‌ها کلیه اطلاعات یک سیستم را هدف قرار می‌دهند.

برنامه‌های مخرب می‌توانند خیلی ساده یا خیلی پیچیده، خیلی کم آزار یا بسیار خطرناک خیلی کند یا بسیار سریع (در انتشار آلودگی) باشند. معمولا پس از آلودگی به یکی از دسته برنامه‌های مخرب، کاربر متوجه این موضوع نخواهد شد و پس از یک سری اتفاقات تعجب بر انگیز کاربر از عملکرد سیستم متوجه وجود برنامه مخرب خواهد شد. این دسته از برنامه‌ها خود شامل چندین نوع برنامه است که عبارتند از:

۱) ویروس‌ها

شایع‌ترین و مشهورترین نوع از برنامه‌های مخرب، ویروسها هستند که تقریبا همه ما با آنها آشنا هستیم و یا حداقل در رسانه‌ها، خبرهای مهم آن به گوش ما رسیده است. اما ماهیت ویروس چیست؟ ویروس یک برنامه کامپیوتری است که توسط یک یا گروهی از برنامه‌نویسان نوشته شده است و معمولا خود را به هر برنامه قابل اجرایی می



چسباند و منتشر می کند.

ویروسهای کامپیوتری بدین دلیل ویروس نامیده می‌شوند که دارای برخی ویژگی‌های همسان با ویروسهای بیولوژیکی هستند. دلیل نامگذاری این برنامه‌ها به ویروس به چند دلیل است:

در حقیقت، ویروس جزئی از ساختار DNA محسوب می‌شود که در داخل یک غلاف محافظ قرار دارد و بر خلاف سلول‌های زنده نمی‌تواند تکثیر خودبخودی داشته باشد. در عوض، ویروس ساختار DNA خود را به درون یک سلول زنده تزریق نموده و با استفاده ساختار آن به تکثیر و انتشار می‌پردازد. ویروس‌های کامپیوتری نیز نیازمند یک میزبان (برنامه) جهت اجرا شدن هستند تا بتوانند اعمال خود را انجام دهند. و هر دوی آنها تاثیر منفی در زندگی میزبان خواهند داشت.

ویروسهای کامپیوتری همانند ویروس‌های بیولوژیکی می‌توانند خود را تکثیر کنند، بعد از تکثیر میزبان خود را آلوده سازند و پس از ارتباط و اجرای برنامه ویروسی شده، ویروس را به برنامه‌های دیگر منتقل کنند.

با اجرای برنامه، فعالیت ویروس نیز آغاز شده و شروع به آلوده ساختن دیگر برنامه‌ها و انتشار خود می‌کند.

اولین و عمومی‌ترین نوع ویروس‌ها، ویروس‌هایی هستند که تمام برنامه‌ها را آلوده می کنند. لازم به ذکر است که این نوع ویروس‌ها فقط فایل‌هایی اجرایی را آلوده می‌کنند. برای مثال فایلهایی با پسوند EXE، COM در سیستم عامل Dos و فایل‌هایی از این قبیل در سیستم‌های عامل دیگر.

یک ویروس کامپیوتری نیز از طرق مختلفی ممکن است وارد کامپیوتر شود و ممکن است تا مدتها به فعالیت خود ادامه داده و پس از مدتی اختلالاتی را در کامپیوتر ایجاد نماید.

۲) بمب‌های منطقی

این دسته از برنامه‌ها همانند کلیه برنامه‌های مخرب دیگر باعث خرابی در یک سیستم می‌شوند اما معمولا این خرابی را فقط در یک زمان خاص (تاریخ یا ساعت) انجام می‌دهند از خطرناکترین بمب‌های منطقی دهه اخیر می‌توان به چرنوبیل اشاره کرد که در روز فاجعه چرنوبیل باعث خرابی نرم‌افزارها و حتی بعضی از سخت‌افزارها می‌شود.

۳) کرمها

این برنامه‌ها بدون در نظر گرفتن فایل عمل خرابکاری خود را انجام می‌دهند، برخلاف ویروسها، کرمها به دنبال آلوده

فایل‌های ضمیمه ممکن است حاوی ویروس باشند. متاسفانه نامه‌های الکترونیکی بدون ضمیمه نیز می‌توانند حاوی ویروس باشند.

راه‌های پیشگیری از آلوده شدن به برنامه‌های مخرب

استفاده از یک برنامه ضد ویروس: (Anti Virus)

یکی از روشهای جلوگیری از انتقال ویروس (برنامه‌های مخرب) به کامپیوتر و حذف ویروس‌ها از کامپیوتر استفاده از نرم افزارهای ضد ویروس است. نرم افزارهایی هستند که فایلهای آلوده ویروس را شناسایی کرده و ویروس را از روی کامپیوتر حذف می‌کنند. از معروفترین و متداولترین نرم افزارهای ضد ویروس می‌توان به آنتی ویروس‌های زیر اشاره کرد:

Norton Antivirus - MacAfee Virus Scan - Panda Antivirus – Kaspersky – Bit Defender

پیشگیری از آلوده شدن به ویروس‌های اینترنتی

- از یک آنتی‌ویروس معتبر استفاده نمایید.
- نامه‌های الکترونیکی مشکوک را بدون بازکردن حذف کنید.
- ضمیمه‌های نامه‌های الکترونیکی ناشناس را اجرا نکنید. اگر ضمیمه‌ها فایلهای اجرایی با اسناد Word بود بدون بررسی توسط نرم افزارهای ضد ویروس آنها را اجرا نکنید.
- از دریافت Activexها بدون امضاء یا اصطلاحاً Unsigned خودداری کنید. Activexهایی را دریافت کنید که امضاء شرکت VeriSign را داشته باشند. امروزه اکثر سایتها برای Activexهای مورد استفاده خود از شرکت VeriSign امضاء دیجیتالی گرفته و اعتبار صحت Activex را از این شرکت دریافت می‌کنند.
- از دریافت Appletها از سایتهای ناشناس خودداری کنید.
- در دریافت و اجرای فایلهای با پسوند XLS, DOC, PIF, COM, EXE دقت کنید. قبل از اجرای این فایلهای حتماً آنها را با نرم افزارهای ضد ویروسی بررسی کنید.
- از سایتهای ناشناخته و مشکوک فایل اجرایی دریافت نکنید .هرگاه با دنبال یک نرم افزار خاص بودید از سایتهای معروف نظیر http://www.download.com یا سایت

ویژه همان نرم افزار استفاده کنید.
- بدلیل تولید ویروسهای جدید، آنتی ویروس خود را با آخرین نسخه‌های نرم‌افزاری ارائه شده بروز رسانی نمایید.

چند نکته امنیتی

- **Back-up گرفتن منظم از اطلاعات ارزشمند موجود بر روی کامپیوتر:**

در فواصل زمانی مشخص و بر اساس یک برنامه خاص از اطلاعات ارزشمند موجود بر روی کامپیوتر Back-up گرفته شده و آنان را بر روی رسانه‌های ذخیره سازی نظیر لوحهای فشرده ذخیره نمایید.

- **دریافت و نصب منظم Patchهای به هنگام شده مربوط به نقایص امنیتی:**

نقایص امنیتی به صورت مرتب در سیستم‌های عامل و برنامه‌های کاربردی کشف می گردد. شرکت‌های تولید کننده نرم افزار، به سرعت اقدام به ارائه نسخه‌های به هنگام شده‌ای با نام Patch نموده که کاربران می بایست آنان را دریافت و بر روی سیستم خود نصب نمایند. در این رابطه لازم است به صورت منظم از سایت‌های مربوط به تولیدکنندگان نرم افزار بازدید به عمل آورده تا در صورت ارائه Patch آن را دریافت و بر روی سیستم نصب نمود.

- **عدم اشتراک منابع موجود بر روی کامپیوتر با کاربرانی که هویت آنان نامشخص است:**

سیستم عامل نصب شده بر روی یک کامپیوتر، ممکن است امکانات به اشتراک گذاشتن برخی منابع موجود نظیر فایل‌ها را با سایر کاربران شبکه، فراهم نماید. ویژگی فوق، می تواند زمینه بروز تهدیدات امنیتی خاصی را فراهم نماید. بنابراین می بایست نسبت به غیرفعال نمودن ویژگی فوق، اقدام لازم صورت پذیرد.

در خاتمه می‌توان عنوان کرد که داشتن یک آنتی‌ویروس که همیشه در حال بروز رسانی است به همراه رعایت نکات امنیتی دیگر می تواند تا حدود زیادی ما را از آلودگی به ویروسهای کامپیوتری مصون نگه دارد. اما باید همواره این مسئله را مدنظر قرار داد که: هیچ وقت در انتهای نقطه امنیتی قرار نداریم و باید همیشه در حال افزایش و بهبود امنیت قدم برداریم.

ادامه دارد.....

سازی از طریق شبکه هستند. بدین صورت که در محیط شبکه و با استفاده از شکافهای امنیتی آن خود را انتشار می‌دهند به همین دلیل معمولا کرمها توسط نامه‌های اینترنتی تکثیر و پخش می‌شوند. معمولترین راه گسترش یک کرم این است که خود را به همه آدرسهای email ای که شما در address book خود لیست کرده‌اید برساند. نرم‌افزار Outlook شرکت مایکروسافت برنامه email‌ای است که بیشترین آسیب پذیری را در برابر حمله کرمها دارد، فقط به این دلیل که عمومی‌ترین برنامه است.

۴) تروجان

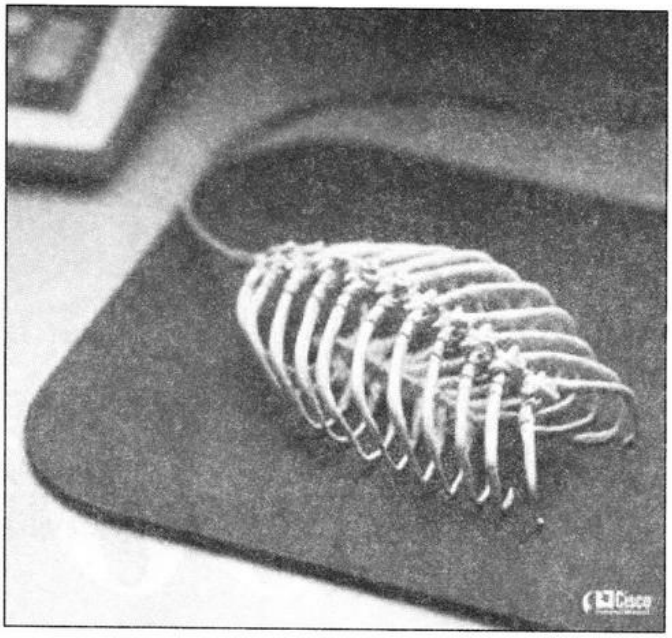
نامگذاری این دسته از برنامه‌های مخرب به تروجان به یونان باستان می‌رسد، زمانی که یونانی‌ها با روم وارد جنگ معروف تروا شدند. در جنگ تروا یونانی‌ها اسبی را به عنوان هدیه به فاتح جنگ هدیه دادند و در شباهنگام سربازان از اسب چوبی پایین آمده و شهر تروا را تسخیر کردند. عنوان تروجان نیز به همین دلیل به تعدادی از برنامه‌ها داده شده که دارای ظاهری زیبا هستند اما در پشت صحنه در حال خرابکاری و ایجاد اختلال در سیستم می باشند. تروجان می‌تواند یک محافظ صفحه نمایش یا یک بازی و ... باشد. خوشبختانه این نوع برنامه‌ها بطور خودکار تکثیر و یا انتشار نمی‌یابند.

۵) ویروسهای نهان

این دسته از ویروسها با استفاده از تغییر مداوم سایز برنامه خودشان را از دید برنامه‌های ویروس‌یاب مخفی نگه می‌دارند و حتی خود را بصورت موقت از روی فایلهای آلوده پاک می‌کنند و یک کپی از خود را بر روی برنامه‌های دیگر در درایوهای دیگر سیستم قرار می‌دهند تا از دید ویروس‌یابها مخفی بمانند.

۶) اسکریپتها

این دسته از برنامه‌ها مخرب به صورت اسکریپتهای یکی از برنامه‌های مجموعه Office معمولا دیده می‌شوند. معمولا این برنامه‌ها به صورت اسکریپتهایی در فایلهای Word یا Excel دیده می‌شوند. خوشبختانه تا زمانی که این فایلها را باز نکرده باشید اسکریپت اجرا نخواهد شد. اما به دلیل



مخفی شدن در فایلهای فوق باید بسیار محتاطانه با این نوع فایلها برخورد نمود.

روشهای انتقال برنامه‌های مخرب (انتشار آلودگی)

انتقال از طریق دیسکت یا سی دی آلوده

بعضی از ویروس‌ها با چسبیدن به انتهای فایلهای اجرایی (با پسوند EXE و COM)، با قرار گرفتن روی سکتور دیسک یا بخش اطلاعات پارتیشن خود را بر روی کامپیوتر منتقل می‌کنند. با اجرای فایل‌های آلوده یا با قرار دادن دیسکت آلوده در کامپیوتر و استفاده از آن، ویروس به کامپیوتر منتقل شده و فعالیت خود را آغاز می‌کند.

انتقال ویروس از طریق شبکه محلی:

هرگاه یکی از کامپیوترهای شبکه محلی بخصوص کامپیوتر Server به ویروس آلوده باشد، ممکن است ویروس از طریق شبکه همه کامپیوترها را آلوده کند. بعضی از ویروس‌ها مخصوص شبکه هستند و ابتدا کامپیوتر سرور را آلوده می‌کند سپس توسط کامپیوتر سرور، کلیه کامپیوترهای شبکه را آلوده می‌سازند. این اتفاق زمانی پیش خواهد آمد که کلیه سیستمها دارای حداقل یک پوشه به اشتراک گذاشته شده باشند. که متاسفانه تعدادی از مدیران شبکه این موضوع را رعایت نمی‌کنند.

انتقال ویروس از طریق اینترنت

با گسترش استفاده از اینترنت، ویروس‌های اینترنت به عنوان نسل جدیدی از ویروس‌های مطرح شدند. ویروس‌های اینترنتی بسیار سریعتر از ویروس‌های دیگر در سطح دنیا انتشار می‌یابند، به صورتیکه ظرف چند روز میلیونها کامپیوتر در سراسر دنیا به یک ویروس جدید آلوده می‌شود. این نوع ویروس‌ها ممکن است از طریق E-MAIL، قطعات نرم افزاری مانند ActiveXها و یا از طریق صفحات وب و غیره به کامپیوتر منتقل شوند.

همانطور که می‌دانیم به همراه برنامه‌های الکترونیکی می‌توان فایلهایی را به صورت ضمیمه ارسال نمود. این