امنیت اطلاعات (قسمت دوم: برنامه های مضر)

مولف: مهدی ریزوندی

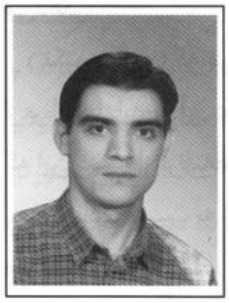
تمامی حقوق مادی و معنوی این اثر متعلق به مهدی ریزوندی بوده و هر گونه استفاده و نشر این اثریا بخشی از آن بصورت مجزا با ذکر نام منبع بلامانع می باشد.

برای کسب اطلاعات بیشتر به وب سایت شخصی مهدی ریزوندی مراجعه فرمایید.

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

امنیت اطلاعات

قسمت دوم: برنامه‌های مضر



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

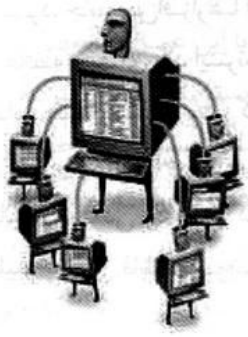
در قسمت اول از مجموعه "امنیت اطلاعات" در خصوص برنامه‌هایی که عملا تخریب اطلاعات را انجام می‌دهند صحبت شد. در این قسمت هدف تمرکز بر برنامه‌هایی است که معمولا هیچ گونه تخریبی بروی اطلاعات انجام نمی‌دهند بلکه به صدد استفاده یا می‌توان بهتر گفت سو استفاده از آن برمی‌آیند. بطور کلی می‌توان این دسته از برنامه‌ها را برنامه‌های مضر نامید.

این برنامه‌ها همیشه جهت ضرر رسانی به گیرنده برنامه مورد استفاده قرار نمی‌گیرند بلکه عموما از سیستم شما به عنوان یک سیستم حمله کننده به سایتهای مختلف استفاده می‌کنند. بدین طریق که برنامه خاص بدون اطلاع کاربر بروی سیستم نصب گردیده و در زمان مقرر (گرفتن دستور از فرد هک کننده) حمله ای را ایجاد می‌نماید.

این حمله با توجه به انتشار برنامه در شبکه اینترنت، قدرت خواهد گرفت و هر مقدار که سیستم ها آلوده شده باشند حمله به سایت مورد نظر فرد هک کننده، قویتر و با شدت بیشتری اتفاق خواهد افتاد. متاسفانه بدلیل اینکه این حمله از طریق سیستمهای بسیار زیادی در اینترنت صورت می‌گیرد، سایت مورد نظر به سختی می‌تواند یک حمله را تشخیص دهد، زیرا از کامپیوترهای بسیار زیادی درخواست اطلاعات دریافت شده است، به همین دلیل این حمله می‌تواند به عنوان یک ترافیک بسیار بالا برای سایت تلقی شود یا حتی خبر خوشحال کننده ای برای مدیران آن سایت باشد، که بر خلاف این تصور پس از چند دقیقه، دیگر سایت قادر به جوابگویی به درخواستهای کاربران واقعی نمی باشد. و این به معنی عدم دسترسی به سایت مورد نظر یا به اصطلاح عدم دریافت سرویس‌های سایت است که می‌تواند هزینه های جبران ناپذیری را برای مشتریان و مدیران سایت ایجاد نماید.

در شبکه‌های جدیدی که به آنها *bot* گفته می‌شود، قربانیان کامپیوترهای خود را توسط برنامه‌ای که هکر بدون اطلاع بروی سیستم نصب نموده، در اختیار هکر قرار داده اند. این فرد با برنامه خود می‌تواند به کلیه سیستم ها نفوذ کرده و دستوری را برای همه سیستم ها ارسال نماید.

این دستور توسط برنامه نصب شده که به آن *zombie* یا "مرده زما" گفته می‌شود



دریافت شده و اجرا می‌گردد. در نظر بگیرید اگر این دستور خاموش نمودن سیستم باشد چه اتفاقی در دنیا رخ خواهد داد. هدف از ایجاد این شبکه ها ارسال دستور "تقاضای اطلاعات" به یک سایت است که نتیجه آن یک حمله همه جانبه و در نتیجه از کار افتادن سرویسهای یک سایت است.

متاسفانه شرکتهایی برای از پا درآوردن شرکت رقیب این شبکه ها را برای مدت زمان کوتاهی اجاره می‌نمایند. برای نمونه می‌توان به شرکت *authorize.net* (ارائه کننده سرویس های پردازش آنلاین کارت اعتباری) که برای مدتی سرویس های آن برای مشتریان قطع شده بود و زیان مالی فراوانی برای شرکت ایجاد نمود، اشاره کرد.

بر خلاف برنامه‌های مخرب که عموماً برنامه‌های عنوان شده هدفشان تخریب اطلاعات بود و کاربر بر اساس تخریب اطلاعات می‌توانست نتیجه گیری نمایید که سیستمش آلوده به یک ویروس است، نمی‌توان به راحتی متوجه این حمله زیرکانه شد. عموماً پس از آلودگی به این دسته از برنامه‌ها، سیستم شما هیچ خطایی محسوسی در کارکرد، انجام و اجرای برنامه‌های روزمره، دستیابی به اینترنت و ... ندارد بلکه در یک زمان خاص حمله تبلیغاتی، سرقت اطلاعات و ... را انجام

Mehdi Rizvandi personal web site's: http://mRizvandi.com Email: mailto:info@mrizvandi.com mrizvandi@yahoo.com

می‌دهد.

نکته دیگری که در خصوص این دسته از برنامه‌ها باید به آن دقت شود، این است که این دسته از برنامه‌ها عموماً اثر تخریبی بسیار زیادی نسبت به برنامه‌های مخرب مانند ویروسها دارند، به این دلیل که درصورت آلوده شدن به یک ویروس و تخریب اطلاعات، می‌توان از نسخه پیشتیبان گرفته شده استفاده نمود، در صورتی که پس از سو استفاده از اطلاعات سرقت شده، دیگر هیچ نسخه پشتیبانی نمی‌تواند به شما کمک کند.

دسته‌ای از برنامه‌های مضر که بشدت استفاده از آن توسط گروه‌های خاصی صورت می‌گیرد، جهت اقداماتی مانند ارسال برنامه‌های آلوده، برنامه‌های تبلیغاتی، برنامه شماره گیر شبکه و ... کاربرد دارد.

معرفی تعدادی از برنامه‌های مضر

۱- برنامه‌های جاسوسی (*Spyware*) جاسوس‌افزار

هر برنامه ای که به جمع آوری اطلاعات کاربران یا سازمانهای متصل شده به اینترنت بدون اطلاع کاربر بپردازد برنامه جاسوسی قلمداد می‌شود. این دسته برنامه‌ها معمولا اطلاعات کاربر را جهت استفاده های تبلیغاتی بکار می‌برند. برنامه‌های جاسوسی معمولا با برنامه‌های رایگان یا آزاد که در اینترنت پخش می‌شوند ترکیب شده اند (هر چند که در آن سایت عنوان شده باشد که برنامه مذکور دارای جاسوس‌افزار یا تبلیغ افزار نیست). البته کلیک بروی تبلیغ برنامه‌ای که در اینترنت معرفی شده بدون اطلاع کافی از آن یا تبلیغ و نصب توسط نرم افزار های دیگر نیز راه دیگری برای ورود جاسوس‌افزارها به سیستم شماست. اولین حمله گسترده این برنامه‌ها در سال ۱۹۹۹تحت یک بازی به نام *Elf Bowling* صورت گرفت. جاسوس‌افزارها از این نظر که بدون اطلاع کاربر بروی سیستم قرار می‌گیرند مشابه اسب های تروا هستند.

در دنیای نرم افزار، جاسوس‌افزار به تنهایی به عنوان یک برنامه خطرناک شناخته نمی شود، زیرا این برنامه به عنوان یک برنامه‌های عمومی عرضه می‌شود. بسیاری از کاربران اینترنت با نصب این برنامه‌ها و مشاهده هر تبلیغ، مبلغی را از ارائه دهنده برنامه دریافت می‌کنند. ولی امروزه رایج ترین روش حمله به سیستم‌ها، سواستفاده از این نوع برنامه‌ها است.

روش کار این برنامه به این شکل است که برنامه پس از نصب بدون اطلاع کاربر، تمامی عملیات کاربر در خصوص اطلاعات ارسالی و دریافتی از اینترنت را مورد بررسی قرار می‌دهد. جاسوس‌افزارها همچنین اطلاعات دیگری در خصوص آدرسهای ایمیل، کلمات عبور، شماره کارت اعتباری و ... را ردگیری می‌نماید.

پس از نصب این برنامه‌ها جاسوس‌افزار نیز بروی سیستم نصب گردیده و مشکلات آغاز می‌شود. جاسوس‌افزارها از منابع سیستم، حافظه و پهنای باند اینترنت جهت ارسال داده ها استفاده می‌کنند. از قابلیتهای این برنامه‌های اجرایی می‌توان به توانایی مانیتور نمودن فشردن کلیدهای صفحه کلید، پویش فایلها، پویش دیگر برنامه‌ها (مانند برنامه‌های گپ زنی، پردازشگر لغات)، نصب برنامه‌های جاسوس‌افزار دیگر، خواندن فایلهای کوکی (*Cookie*) اینترنت و تغییر صفحه پیش فرض اینترنت اشاره نمود. پس از کسب اطلاعات، موارد برای شخص مورد نظر ارسال می‌گردد و از این لحظه به بعد صفحات تبلیغاتی شروع به باز شدن می‌کنند. پس از بازدید شما از یک سایت چندین سایت دیگر باز شده، یا برنامه‌هایی بروی سیستم نصب می‌گردند که شما از نصب آنها اطلاعی ندارید.

البته در زمان نصب بعضی از برنامه‌ها به کاربر اطلاع داده می‌شود که همراه این برنامه یک جاسوس‌افزار نصب خواهد شد، اما به علت عبور سریع و مطالعه ننمودن این صفحه از نصب آن آگاهی پیدا نمی‌کنیم.

● فایلهای کوکی (*Cookie*) جهت ذخیره سازی اطلاعات کاربر در یک سایت بروی سیستم کاربر استفاده می‌شود. معمولا اطلاعات ورود به سایت مانند نام کاربری و رمز عبور جز این اطلاعات هستند (البته اگر کاربر گزینه به خاطر آوردن سایت را کلیک نموده باشد). جاسوس‌افزارها پس از بررسی این فایلها می‌توانند نام کاربر و رمز عبور شما را در سایتهای مختلف بدست آورند.

۲- برنامه‌های تبلیغی (*adware*) تبلیغ افزار*

این دسته از برنامه را می‌توان جاسوس‌افزار خاصی نامید که فقط اطلاعات جمع‌آوری شده را برای نمایش تبلیغات در صفحهات اینترنت بکار می‌برد. آلوده شدن به چنین برنامه ای یعنی باز شدن پیاپی صفحات حاوی تبلیغات و اطلاعات مختلف بدون اجازه کاربر. در چنین شرایطی استفاده از اینترنت به

Mehdi Rizvandi personal web site's: http://mRizvandi.com Email: mailto:info@mrizvandi.com mrizvandi@yahoo.com

حداقل خود خواهد رسید، زیرا ورود به صفحات تبلیغات یعنی سردرگمی در اینترنت و تایید ارائه بیشتر تبلیغات از طرف ارسال کننده.

۳- برنامه‌های مزاحم (*parasiteware*) مزاحم افزار*

برنامه‌هایی که بدون اطلاع و بدون نیاز شما بروی سیستم نصب می‌شوند، اطلاعات شما را برای شخصی ارسال و تغییراتی در برنامه مرورگر اینترنت شما ایجاد می‌نمایند. این برنامه‌ها جستجوی شما را به سایتهای خاص خود ارسال می‌کنند و باعث کند شدن سیستم شما و ارتباط اینترنت می‌شوند. جاسوس‌افزار را می توان یک نمونه از این نوع برنامه‌ها دانست.

۴- برنامه‌های تجسس کننده (*snoopware*)*

این دسته از برنامه‌ها شباهت بسیار زیادی به برنامه‌های جاسوس‌افزار دارد. این برنامه برای مانیتور کردن کارمندان، بچه ها یا والدین بکار می‌رود. تجسس کننده‌ها می‌توانند به حالت نهان بروی سیستم قرار گرفته و تمامی اعمال کاربر از قبیل، تایپ و تصویر مانیتور را پویش نمایند. بسیاری از این دسته برنامه‌ها دارای روالی هستند که اطلاعات کسب شده را به شکل یک ایمیل برای فرد پشت صحنه ارسال می‌نمایند و سپس عملیات تخریبی بر اساس تصاویر و کلیدهای تایپ شده شروع می‌شود.

۵- برنامه‌های (*backdoor*)

برنامه‌هایی که پس از نصب بر روی سیستم قربانی یک راه عبور مخفی در سیستم ایجاد می‌نمایند و از آن طریق برنامه نویس برنامه می‌تواند وارد سیستم قربانی شده و دستورات خود را به اجرا درآورد. بدین طریق، اطلاعات شخصی، داده های حساس و برنامه‌های سیستم در اختیار فرد مهاجم قرار می‌گیرد.

۶- برنامه‌های ثبت کننده ضربات صفحه کلید (*keystroke logger*)*

برنامه ای که تمامی ضربات صفحه کلید (حتی کلیدهای پاک کردن) را ذخیره می‌نماید. هدف این برنامه یافتن رمزهای عبور و پیدا نمودن شماره و رمز کارت اعتباری است.

۷- برجهای راهنما (*web beacon*)*

برجهای راهنما معمولا تصاویری با قالب *gif* هستند و اندازه آنها عموما از ۱×۱ پیکسل بیشتر نیست و بصورت شفاف در ایمیل ها قرار داده می‌شوند. هدف از این کار این است که پس از باز نمودن ایمیل درخواستی از طرف شما (نامحسوس) برای مشاهده تصویر مورد نظر ارسال می‌گردد، سپس سایت ارسال کننده با مانیتور نمودن رفتار شما اطلاعات فراوانی را کسب می‌کند، اولین اطلاع بدست آمده آدرس آی‌پی سیستم شماست که بر اساس آن درخواست ارسال شده است. اطلاعاتی از قبیل مدت زمان مشاهده ایمیل یا وب سایت، زمان مشاهده، نوع مرورگر و اطلاعات درون کوکی ها و ... نیز برای سایت یا فرد ارسال کننده ایمیل ارسال می‌گردد.

۸- بمب صندوق پستی (*mail bomb*)*

ارسال حجم انبوهی از نامه‌ها همراه ضمیمه برای یک مقصد مشخص که باعث پر شدن فضای صندوق پستی گردیده یا حتی باعث پر شدن فضای دیسک سرور می‌شود. با این عمل نامه‌های اصلی در صندوق پستی قرار نمی گیرند یا حتی ممکن است سیستم دچار خطا شود.

۹- نامه‌های ناخواسته (*spam*)*

نامه‌هایی که بدون نیاز برای شما ارسال می‌گردد را نامه‌های ناخواسته می‌گویند. مانند نامه‌های بازرگانی بدون درخواست، نامه‌های گروهی (*Bulk*)، نامه‌های *Gray* و نامه‌های کم ارزش. نامه‌های ناخواسته، برای تبلیغات بازرگانی یک کالا بصورت سیاستمدارانه یا بصورت دسته جمعی برای صندوقهای پستی ارسال می‌گردد. همانند ویروسها میلیونها نسخه از این برنامه‌ها هر روزه در اینترنت ارسال می‌گردد. یک آفت همه جانبه برای کاربران اینترنت. البته عموما تا زمانی که یک نامه ناخواسته *Replay* نگردیده باشد، تقریبا کنترل اوضاع در دست شما خواهد بود. عموما در تمامی نامه‌های ناخواسته های آدرس وب سایتی معرفی می‌گردد، با کلیک بروی این آدرس، اطمینان خاطر برای ارسال کننده بوجود می‌آید که شما خواهان و موافق موضوع نامه هستید و از این لحظه به بعد سیل نامه‌های مختلف برای صندوق پستی شما روانه می‌شود. سوالی که پیش می‌آید این است که چرا ارسال کننده‌گان نامه‌ها این کار را انجام می‌دهند؟ و حتی لیست آدرس صندوق های پستی را می‌فروشند؟ اولین دلیل این موضوع این است که ارسال کننده ایمیل با بدست آوردن یک آدرس ایمیل مبلغی را از فرد درخواست کننده دریافت می‌کنند و فرد درخواست کننده شروع به ارسال موارد مختلف برای آن صندوق پستی می‌نماید. اگر ارسال کننده یک میلیون ایمیل را در یک هفته ارسال نماید، می‌تواند روی مبلغ ۵۰۰ دلار فکر کند. این عمل در کمتر از ۱۵ دقیقه صورت می‌گیرد و این به معنای ۱۰۰,۰۰۰ دلار در سال است. این مبلغ می‌تواند انگیزه مناسبی برای یک بچه دبیرستانی باشد. توجیه این عمل نیز بسیار ساده است، روزانه ما در همه جا و همه مکانی از قبیل روزنامه، تلویزیون، رادیو، اتوبوس و ...

Mehdi Rizvandi personal web site's: http://mRizvandi.com Email: mailto:info@mrizvandi.com mrizvandi@yahoo.com

تبلیغات را می‌بینیم، که هر کدام هزینه‌های فراوانی را نسبت ارسال ایمیل دارند.

راه‌های مقابله با برنامه‌های جاسوس‌افزار و دیگر برنامه‌های مضر

۱- مطالعه پذیرش قرارداد نصب برنامه (*License Agreement*): بدلیل شباهت قرارداد نصب بین برنامه‌ها، این قرارداد معمولا خوانده نمی‌شود، پیشنهاد می‌گردد برنامه‌های ناشناخته را حتما مورد بازنگری قرار داده و از عدم نصب جاسوس‌افزار اطلاع حاصل نمایید.

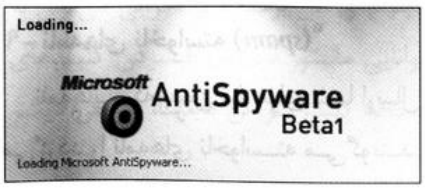
۲- در پاسخ به نصب برنامه از سایتهای مختلف تا زمان اطمینان از سایت مورد نظر و درخواست خود مبنی بر نصب، هرگز گزینه‌های داخلی پنجره را انتخاب ننموده و از دکمه بستن پنجره استفاده نمایید.

۳- برای متوجه شدن از وجود برجهای راهنما در سایتها می‌توان کد صفحه وب را مشاهده نمود و تگهای *IMG* را بررسی نمود، در صورتی که آدرس فایل مربوط به سرور دیگری باشد، امکان وجود یک برج راهنما می‌رود. برای اطمینان از جلوگیری نمودن این دسته از حملات می‌توان، تنظیم دریافت کوکی را غیر فعال نمود تا هیچ کوکی نتواند بروی سیستم شما ذخیره گردد.

۴- یک راه حل بسیار ساده برای جلوگیری از حرکت برنامه‌های مضر، تنظیم حد دسترسی به سیستم است. در صورتیکه حساب کاربری تعریف شده برای شما از نوع کاربران محدود شده باشد، بسیاری از برنامه‌ها نمی توانند بصورت اتوماتیک و بدون اجازه روی سیستم شما نصب شوند. به همین دلیل پیشنهاد می‌شود حساب

کاربری تعریف شده خود را همیشه در حداقل حقوق دسترسی قرار دهید. در سیستم های خانگی در هر زمان که کاربر نیاز به حقوق دسترسی ویژه ای داشته باشد می‌تواند از حساب کاربری سطح بالاتری یا حتی از حساب کاربری مدیر سیستم (*Administrator*) استفاده نماید. در شبکه های محلی که معمولا در ادارات و شرکتها کاربرد دارد نیز پیشنهاد می‌گردد، حساب کاربری کلیه پرسنل اعم از مدیر، رییس و کارمند از نوع حساب کاربری محدود شده باشد (*Domain user*) و هر زمانی که کاربر نیاز به حقوق دسترسی ویژه ای داشت از مدیر شبکه کمک بگیرد. با این روش بسیاری از مشکلات نصب برنامه‌های مضر در شبکه های محلی نیز رفع می‌شود.

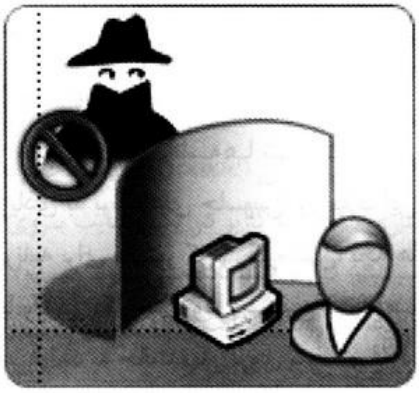
۵- استفاده از یک برنامه ضدجاسوس‌افزار نیز کمک فراوانی در پیشگیری از آلودگی به برنامه‌های مضر خواهد نمود. برای نصب این نوع برنامه‌ها حتما از صحت عملکرد و عملیات برنامه مورد نظر آگاهی لازم را بدست آورید سپس برنامه را نصب نمایید. تعدادی از برنامه‌های ضد جاسوس‌افزار خود یک جاسوس‌افزار حرفه ای هستند پس مراقب انتخاب خود باشید. پیشنهاد می گردد از



برنامه *Microsoft Antispy* یا نسخه جدید این برنامه به نام *Windows Defender* استفاده نمایید.

۶- نصب یک برنامه دیواره آتش بر روی دستگاه دروازه اینترنت (*gateway*) کمک بسیار بزرگی برای پیشگیری از حملات از طریق اینترنت می تواند باشد. (دیواره آتش برنامه ای است که مانع از ورود و دسترسی به منابع داخلی سیستم ها می گردد. این برنامه می تواند بروی یک کامپیوتر یا یک سخت افزار خاص نصب گردیده باشد).

۷- استفاده از برنامه ضد نامه‌های ناخواسته در جلوگیری از مشکلات ایمیل کمک بسیار شایانی می‌تواند باشد. البته



اکثر ارائه دهندگان سرویس پست الکترونیک بروی سرویسهای خود برنامه‌های ضد نامه‌های ناخواسته را نصب می نمایند. اما در کنار آن در صورت استفاده از نرم‌افزار *Outlook* می توان این برنامه را نیز بروی سیستم نصب نمود.

در آخر خاطر نشان می نماید که با وجود این تهدیدات، وجود یک ضدجاسوس‌افزار در کنار برنامه ضد ویروس از اهمیت فراوانی برخوردار است و با نصب آن بروی سیستم می‌توان تا حد زیادی از خطرات و مضرات برنامه‌های مضر در امان بود.

ادامه دارد ...

* : ترجمه توسط مولف ارائه شده است

Mehdi Rizvandi personal web site's: http://mRizvandi.com Email: mailto:info@mrizvandi.com mrizvandi@yahoo.com