بدافزار چیست؟

10 قدم اساسی برای حفظ امنیت رایانه

نویسنده

حامد موثق پور

فهرست

Malware یا بدافزار دقیقاً چیست و چگونه از آن پیشگیری نماییم؟

دنیای شبکه و اطلاعات گستردگی فراوانی پیدا کرده است و امروزه تعداد کاربرانی که از طریق مختلف به شبکه جهانی اینترنت متصل هستند سریعاً به درصد بزرگی از جمعیت کل جهان نزدیکتر میشوند. همانگونه که در مکانهای شلوغ و عمومی بیشتر مراقب اموال و اطلاعات خود هستید لازم است که محیط هایی که به یک شبکه بزرگ (مانند اینترنت) متصل است و یا حتی محیط هایی که تردد زیادی در آنها وجود دارد (مانند کامپیوترهای عمومی) را بهتر بشناسید و از امنیت آنها آگاه تر باشید تا اطلاعات شما مورد سرقت واقع نشود و یا درگیر مشکلات عمیق و پیچیده نرم افزاری نشوید.

نرم افزارهای امنیتی زیادی برای محافظت از سیستم عامل های موجود ساخته شده اند. انواع فایروال ها و آنتی ویروس ها از این نوع هستند. این نرم افزارها تا حد زیادی می توانند شما را از خطرات مصون بدارند. ولی درصورتی که می خواهید مانند یک حرفه ایی سیستم عامل خود را زیر نظر داشته باشید بهتر است که اطلاعات بیشتری در مورد بدافزارها ، انواع آنها ، اهداف آنها و نحوه انتشار آنها داشته باشید. حرفه ایی ها به جیا اینکه خود را درگیر پاکسازی رایانه اش از بدافزارها کنند سعی می کنند از آلوده شدن به آنها **پیشگیری** نمایند.

در این آموزش تلاش می کنیم تا این اطلاعات را بصورت طبقه بندی شده و منظم در اختیار شما قرار دهیم. با ما همراه باشید.

بدافزار برگردان فارسی کلمه Malware می باشد. Malware یک کلمه ترکیبی است که از دو کلمه Malicious به معنای **بدخواهانه** و Software به معنای نرم افزار گرفته شده است. ظاهر این عبارت دقیقاً مشخص می کند که ماهیت آن چیست. بدافزار ها نرم فزارهای ناخواسته ایی هستند که معمولاً بدون اجازه صاحب سیستم نصب می شوند و به انجام اعمال ناخواسته یا بدخواهانه روی سیستم می پردازند.

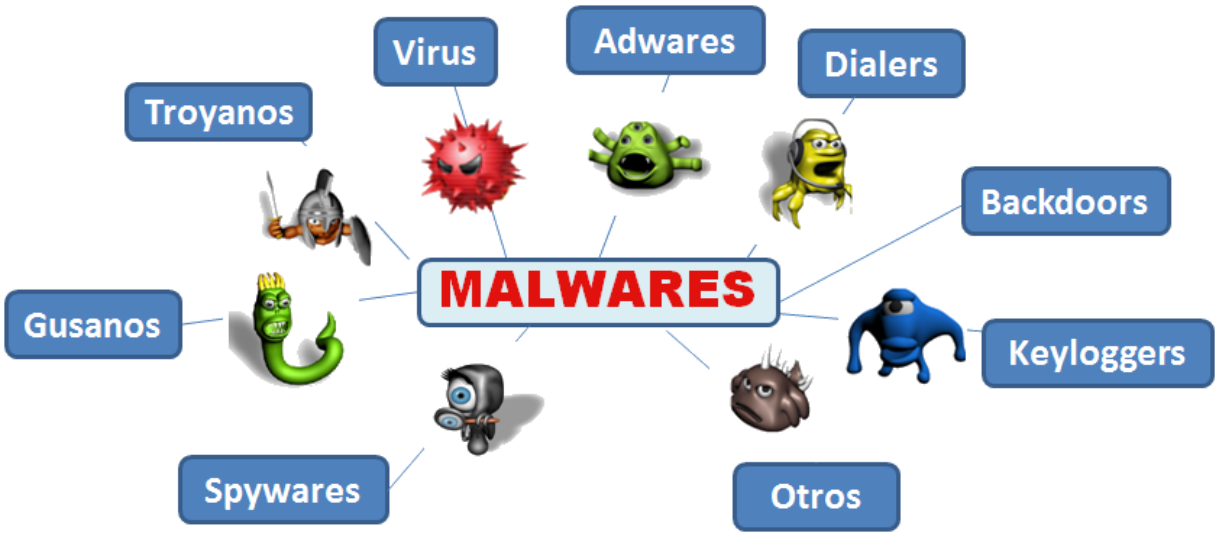
حتماً تا کنون واژه هایی مانند ویروس ، تروجان ، کرم و مانند اینها را شنیده اید. در حقیقت همه ی اینها نوعی از بدافزارها هستند.

بدافزارها را لحاظ نوع عملکرد می توان در دو دسته کلی قرار داد:

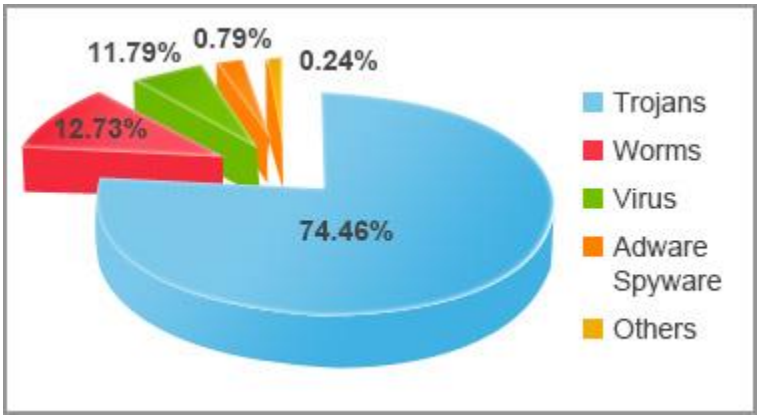
- بدافزارهایی که بصورت مستقل و بدون نیاز به برنامه ی دیگری روی سیستم عامل می توانند اجرا شوند.
- بدافزارهایی که برای اجرا نیازمند میزبان خود هستند و به تنهایی نمی توانند فعالیت نمایند.

جالب است بدانید اولین بدافزارها از نوع **ویروس** بودند که در سال 1980 با هدف خرابکاری در اطلاعات ذخیره شده روی کامپیوترها نوشته شدند. بعد از آن اولین **کرم اینترنتی** (**Internet Worms**) در سال 1988 بوجود آمد که هدف اصلی آن آلوده کردن سیستمهای SunOS و VAX BSD بود. این کرم، از طریق یک آسیب پذیری شبکه ای در این سیستم عامل ها، به آن ها حمله کرده و بعد از نفوذ، برنامه مخربی را روی سیستم اجرا می کرد.

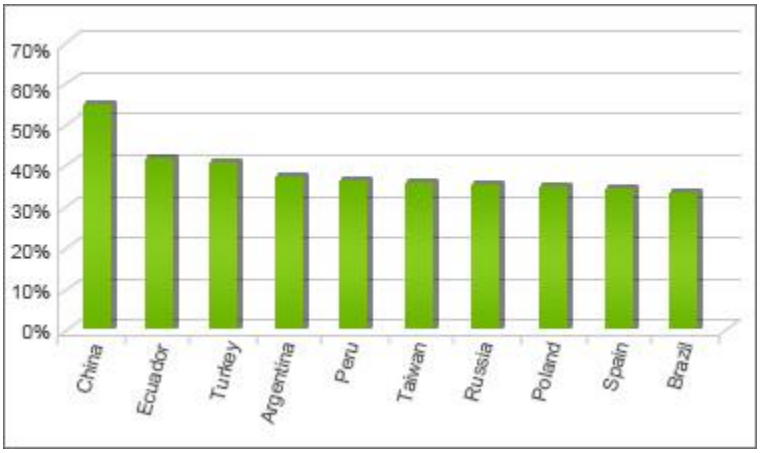
در اوایل سال 2000 کم کم نوع خرابکاری ها عوض شد و به سودجویی هایی منجر شد که هدف اصلی آنها سوء استفاده از کامپیوترها به عنوان **Zombie** بود. بعد از آن نرم افزارهای **در پشتی** (**Backdoor**) بصورت گسترده ایی رواج یافت. از سال 2003 به بعد بدافزارهای **جاسوسی** نیز مشتاقان زیادی پیدا کرد و دزدی اطلاعات به شدت محبوب گردید.



در این تاریخچه کوتاه متوجه شدید که بدافزارهای انواع گوناگونی دارند و در مقاطع زمانی تغییراتی داشته اند که با توجه به نوعشان نام هایی به خود اختصاص داده اند. غیر از نام هایی که ذکر شد بدافزارهایی به نام های **Spyware**، **Rootkit** ، **Hack Tool** ، **Adware** ، **Logic** ، **Bomb**، **Bacteria** ، **Scareware** نیز وجود دارند.



در دوره های زمانی خاص تعدادی از بدافزارها گسترش بیشتری پیدا می کردند. طبق آماری که موسسه امنیتی پاندا سال گذشته منتشر کرد **تروجان ها** رکورد دار بدافزارها بودند. این موسسه با بررسی یک نمونه 6میلیون نیمی از بدافزارها اعلام کرد قریب به 80 درصد از کامپیوترهای دنیا در سال 2013 به تروجان ها آلوده شده اند.



طبق بررسی موسسه فوق به ترتیب کشورهای چین ، اکوادور ، ترکیه ، آرژانتین ، پرو ، تایوان ، روسیه ، لهستان ، اسپانیا و برزیل بیشترین سهم را در آلوده شدن به بدافزارها به خود اختصاص داده اند.

در سری آموزشی **امنیت ویندوز** با انواع بدافزارها آشنا خواهید شد و می آموزید چگونه از آلوده شدن به آنها پیشگیری نمایید و در صورت آلوده شدن چگونه رایانه خود را از آنها پاکسازی نمایید.

ویروس چیست و چگونه از آلوده شدن به آن پیشگیری نماییم؟

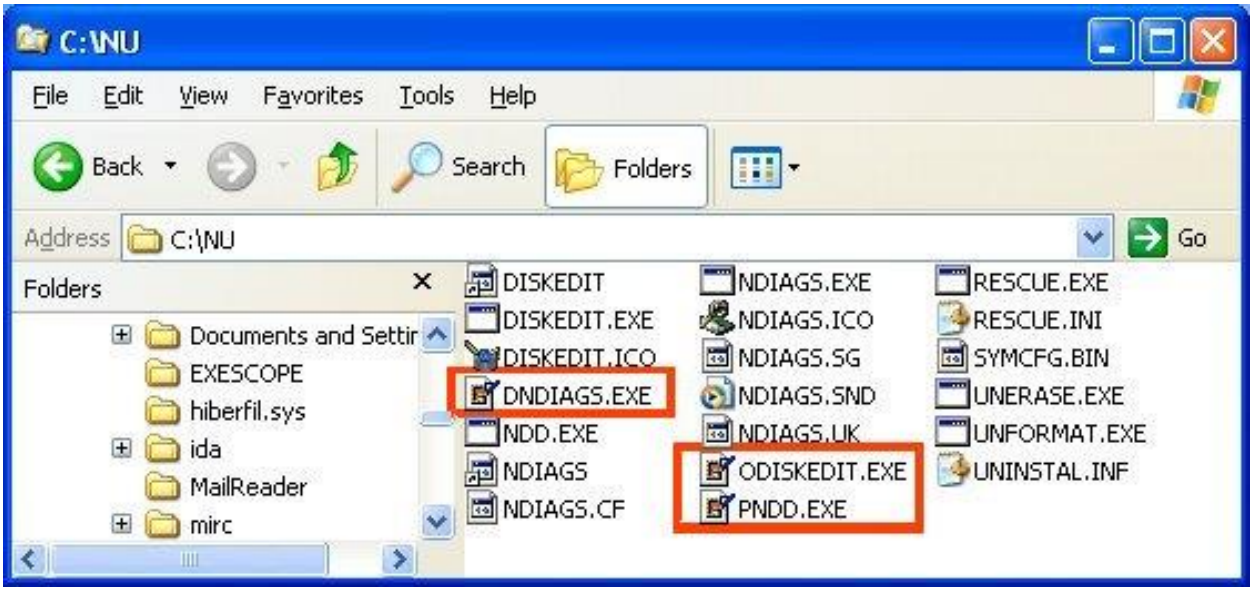
وقت آن رسیده است که بصورت دقیق تر با هر کدام از انواع بدافزارها آشنا شویم و نحوه شیوع آنها و جلوگیری از آلوده شدن سیستم عامل رایانه مان به آنها را فرا بگیریم.

ویروس (virus)

ویروس ها نوعی از بدافزارها هستند که به دلیل گستردگی ای که پیدا کرده اند، هر نوع بدافزاری به این لفظ شناخته می شود.

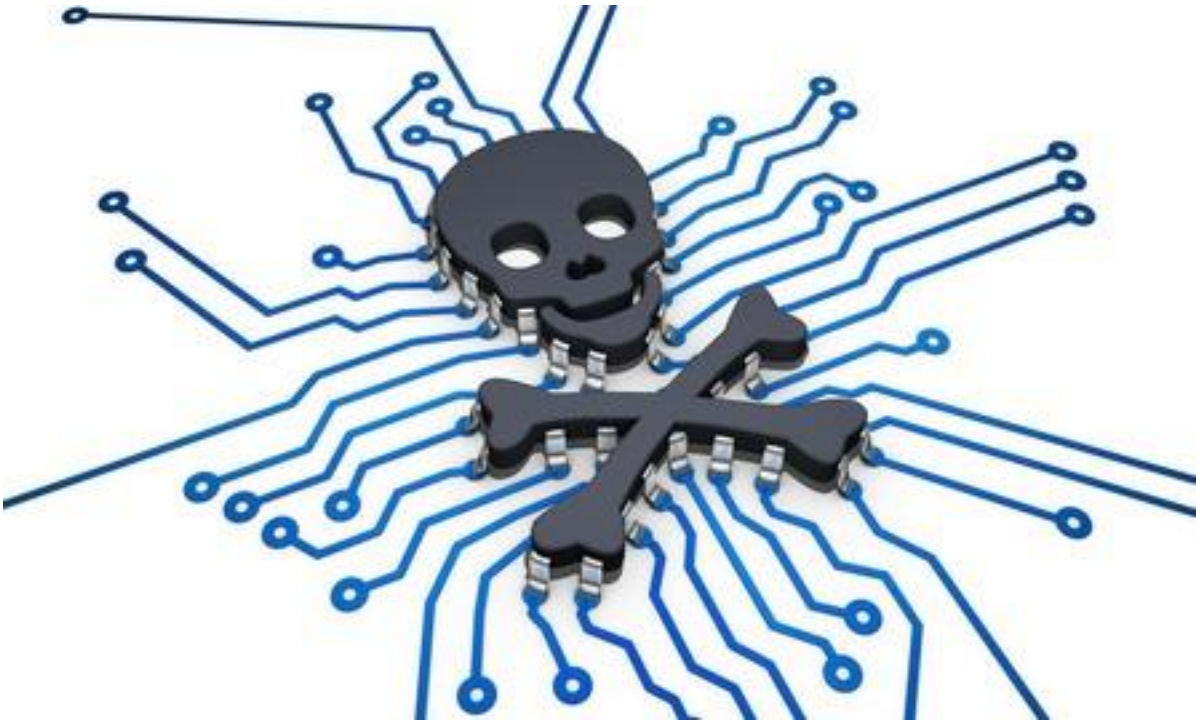
این نوع بدافزارها به دلیل نوع فراگیر شدن و شیوع آنها به این نام (ویروس) معروف شده اند. خصوصیت اصلی ویروس ها خود تکثیر (Replicate) بودن آنها است. نام گذاری این نوع بدافزارها به نام ویروس به دلیل شباهت بسیار زیاد آنها به ویروس‌های بیولوژیک می باشد. این نوع بدافزارها همانند ویروس‌های بیولوژیک از میزبانی به میزبان دیگر منتقل می شوند.

ویروس ها خود را به برنامه ها و فایلهای اجرایی می چسبانند و همزمان با آنها اجرا شده، فعال و تکثیر می شوند. به همین دلیل ویروس ها تا زمانی که توسط کاربر اجرا نشوند به خودی خود مشکل ساز نیستند.



در ذیل فهرست پسوندهای رایج فایل‌های اجرایی ارائه شده است و اکثر نرم‌افزارهای ضد ویروس در حالت عادی (بدون تنظیمات خاص) این فایل‌ها را ویروس‌یابی می‌کنند (البته در برخی برنامه‌های ضد ویروس ممکن است برخی پسوندها حذف یا اضافه شوند) :

.com ،.exe ،.dll ،.ovl ،.bin ،.sys ،.dot ،.doc ،.vbe ،.vbs ،.hta ،.htm ،.scr
.ocx ،.hlp ،.eml



ویروس ها در ابتدا بیشتر از اینکه به فکر آلوده کردن سیستم باشند به فکر تکثیر خود و جایگیری در محل های از سیستم عامل هستند. ویروس ها دارای برنامه هایی هستند که به محض اجرا شدن به دنبال فایلهایی می گردد که امکان آلوده کردن آنها وجود دارد. پس از آلوده شدن اعمال تخریبی خود را در سیستم عامل دنبال می کنند.

ویروس ها می توانند یک فایل یا کل هارد کامپیوتر شما را پاک کنند و یا سیستم را بطور کامل از کار بیاندازند.

پس ویروس ها به خودی خود هیچ گونه خطری ندارند و برای اجرا نیاز به یک میزبان هستند.توجه به این نکته اساسی میتواند شما را از آلوده شدن به طیف وسیعی از بدافزارها حفاظت نماید:

هرگز فایلهای اجرایی که بطور کامل از ماهیت و سالم بودن آنها اطمینان ندارید اجرا ننمایید.

ویروس ها بعد از فعال شدن به چه اعمالی می پردازند؟

بسیاری از ویروس‌ها دارای اثراتی هستند که هرچند تخریبی نمی‌باشد ولی می‌تواند برای کاربر ایجاد مزاحمت کند. مثلاً ممکن است پیغامی نمایش دهد، باعث ریزش حروف صفحه نمایش به پایین شود یا اینکه یک آهنگ پخش نماید. علاوه بر این برخی از ویروس‌ها به علت اشکالات نرم‌افزاری که ناشی از عدم دقت ویروس‌نویس می‌باشد، ممکن است دارای اثراتی غیرقابل پیش‌بینی باشند که گاهی این اثرات می‌توانند تخریبی نیز باشند. از نقطه نظر کاربر اهمیتی ندارد

که خسارت ایجاد شده بوسیله یک ویروس، یک کار عمدی پیش‌بینی شده توسط نویسنده ویروس بوده باشد یا یک اشتباه برنامه‌نویسی.

برخی از ویروس‌ها در حافظه کامپیوتر مقیم شده و از این طریق عملیات تکثیر خود را انجام می‌دهند. این عمل ممکن است به گونه‌ای باشد که جایی برای اجرای برنامه‌های دیگر نماند و یا باعث ایجاد تأخیر یا وقفه در حین عملیات سیستم اعم از اجرای برنامه‌ها و یا راه‌اندازی کامپیوتر گردد.

ویروس‌ها می توانند اقدام به سرقت اطلاعات و کلمات عبور کاربر کنند. بعضی از اینگونه بدافزارها با مقیم شدن در حافظه از عباراتی که توسط شما تایپ می‌شود گزارش گرفته و پس از اتصال رایانه شما به اینترنت این اطلاعات را برای مقصد خاصی ارسال می‌کنند. گیرنده این اطلاعات می‌تواند به راحتی از آنها سوء استفاده‌های مختلفی نماید.

با وجود اینکه طبق آماری معتبر تنها 5 ردصد ویروس ها دارای اثرات تخریبی هستند ولی هیچ ویروسی کاملاً بی‌ضرر نیست و در خوشبینانه‌ترین حالت، آنها منابع شما و کامپیوترتان را مصرف می کنند.

اثرات تخریبی ویروس ها معمولاً یکی از موارد زیر می باشد:

- تخریب یا حذف برنامه‌ها و اطلاعات بخش‌های مختلف دیسک‌ها
- فرمت کردن دیسک‌ها
- کد کردن اطلاعات و برنامه‌ها
- تخریب اطلاعات حافظه فلش ها

از کجا بفهمیم که کامپیوترمان ویروسی شده است؟

معمولاً هر آسیب یک سری علائم دارد. آلوده شدن به بدافزار ویروس نیز علائمی در پی دارد که مشاهده هر کدام می تواند دلیلی بر ویروسی شدن باشد.

- سیستم در هنگام راه‌اندازی قفل می‌کند و احتمالاً پیغام‌های غیرمعمول روی صفحه ظاهر می‌گردد.
- هنگام اجرای برنامه‌ها پیغام کمبود حافظه ظاهر شده و برنامه اجرا نمی‌گردد.
- در کارچاپگر اختلال ایجاد می‌شود یا بدون هیچگونه فرمان چاپی شروع به کار می‌کند.
- امکان دسترسی به برخی از درایوها وجود ندارد.
- هنگام اجرای فایل‌ها، پیغام File is Damaged یا File is Corrupted نمایش داده می‌شود.
- هنگام اجرای یک فایل، کاراکترها و یا پیغام‌های غیرعادی روی صفحه نمایش ظاهر می‌گردد.
- هنگام کار در محیط‌های گرافیکی، تصاویر به هم می‌ریزد.

- اصوات غیرمعمول یا موزیک از بلندگوهای کامپیوتر پخش می‌شود.
- سیستم هنگام اجرای یک برنامه قفل کرده و حتی گاهی فشردن کلیدهای Ctrl+Alt+Del نیز نمی‌تواند سیستم را دوباره راه‌اندازی کند.
- اطلاعات بخشی از دیسک سخت و یا تمام آن بطور ناگهانی از بین می‌رود یا دیسک سخت ناخواسته فرمت می‌شود.
- اندازه فایل‌های اجرایی افزایش می‌یابد.
- خواص فایل‌های اجرایی تغییر می‌کند.
- سرعت سیستم بطور نامحسوسی کاهش می‌یابد.
- اطلاعات Setup کامپیوتر از بین می‌رود.
- برنامه‌ها مراجعاتی به دیسکت انجام می‌دهند که قبلاً انجام نمی‌دادند.
- کاهش فضای خالی دیسک بدون اینکه فایلی اضافه شده و یا به محتوای فایل‌ها افزوده شده باشد.
- نرم‌افزارهای مقیم در حافظه با خطا اجرا شده یا اصلاً اجرا نمی‌شوند.
- بعضی برنامه‌ها سعی در برقراری ارتباط با اینترنت را دارند.
- هنگام کار با اینترنت مقدار ارسال و دریافت اطلاعات ناخواسته افزایش یافته و سرعت به شدت افت می‌کند.
- نامه‌های الکترونیکی ناخواسته از روی سیستم ارسال شده و یا دریافت می‌گردد.

پاکسازی رایانه آلوده به ویروس

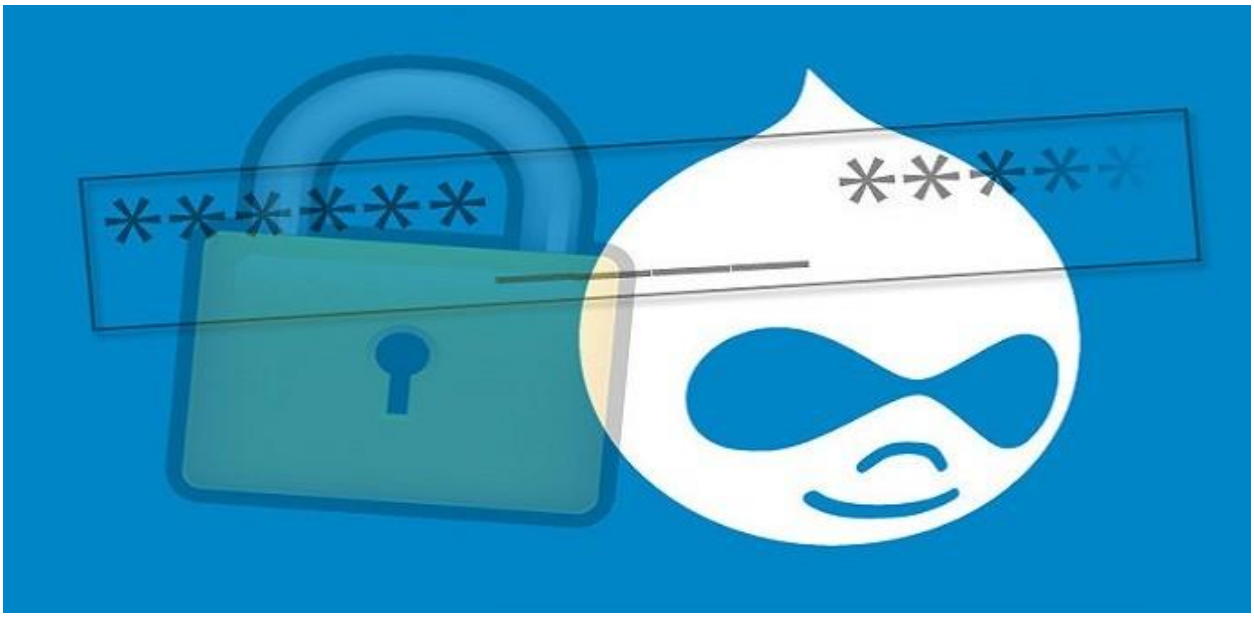
استفاده از یک آنتی ویروس قدرتمند ، بروز رسانی مداوم آن و اسکن کردن کل سیستم بصورت دوره ایی می توان ویروس های معمول را از روی رایانه پاکسازی نمود. در بعضی موارد نیز ویروس ها بسیار پیشرفته هستند و از کار انداختن آنها تا به روز رسانی دیتابیس های نرم افزارهای آنتی ویروس معلق می ماند.

بدافزار در پشتی (Back Door) را جدی بگیریم!

همانگونه که از نام آن معلوم است یک راه نفوذ پیش بینی نشده برای ورود غیر مجاز ایجاد می نماید. درپشتی نوعی بدافزار است که به ظاهر برنامه ایی ساده و سالم است (حتی میتواند یک برنامه ضد ویروس باشد) ولی در شرایطی خاص زمینه ورود و دسترسی مهاجمین به داده های سیستمی که روی آن نصب شده است را مهیا می کند.

درهای پشتی را به سه دسته **فعال**، **غیرفعال** و **حمله بنیان** تقسیم می شوند.

- درهای پشتی‌ای که منتظر رسیدن دستورات از طریق درگاهها می‌شوند را غیرفعال می‌نامند.
- درهای پشتی فعال خودشان آغازگر ارتباط با میزبان‌های دیگر هستند.
- درهای پشتی حمله‌بنیان به درهایی گفته می‌شود که با استفاده از حمله‌ای مبتنی بر کدهای مخرب به دسترسی‌های لازم می رسند.



سیستم مدیریت محتوای وبسایت دروپال یکی از سیستم های حرفه ایی و پرطرفدار در سطح جهان می باشد. به تازگی در این سیستم یه آسیب پذیری امنیتی کشف شده است که نوعی دسترسی به دیتابیس برای هکرها ایجاد میکند. روشی که هکرها دراین نوع آسیب پذیری مورد استفاده قرار داده اند درپشتی (backdoor) می باشد و در منابع خبری آمده است که پیش بینی می شود تا کنون بیش از 12 میلیون وب سایت دروپالی تا الان دارای یک درپشتی شده اند. هکر ها از طریق این در پشتی دسترسی کامل به دیتابیس خواهند داشت و براحتی می توانند یوزر جدید برای آن ایجاد نموده و کل اطلاعات دیبابیس را استخراج نموده یا حذف کنند.

برای جلوگیری از آسیب پذیری از طریق در پشتی توجه به موارد زیر مفید خواهد بود :

- هرگز پیوست های ایمیل های دریافتی از سوی کاربران ناشناس را باز نکنید
- در بسیاری از وب سایت ها (غالباً وب سایت های با موضوع دانلود) کلیدهایی با عنوان دانلود در نزدیکی لینک های واقعی دانلود وجود دارد. حتماً قبل از کلیک کردن روی آنها از هدف آن لینک ها مطمئن شوید (با نگه داشتن ماوس و مشاهده آدرسی که با کلیک کردن به آن هدایت خواهید شد)
- از نصب نرم افزارهای ناشناخته و نرم افزارهایی که نیاز ندارید خودداری کنید و در صورت نیاز به نرم افزار جدید حتماً از منابع تایید شده (مانند وبسایت های رسمی تولید کننده نرم افزار یا وبسایت های شناخته شده در زمینه معرفی نرم افزارها) سورس آنها را تهیه کنید و در صورت عدم آگاهی با اشخاص مطلع مشورت نمایید.

کرم‌ها (worms) چگونه می توانند به کامپیوترها آسیب برسانند؟

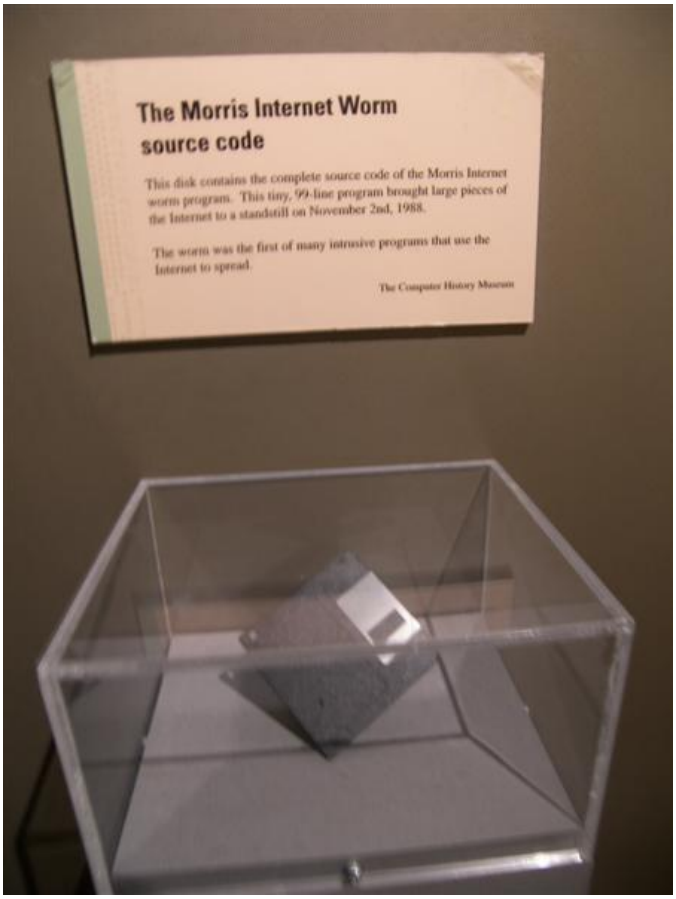
این گروه از بدافزارها در بستر شبکه فعالیت می کنند. و هدف اصلی آنها نفوذ از طریق حفره های آسیب پذیر شبکه به سیستم و آلوده کردن آنها به ویروس و استفاده از سیستم قربانی برای آلوده کردن دیگر سیستم ها.

در واقع کرم ها در بستر شبکه خود را به زور به سیستم کاربر می رسانند و اهداف سودجویانه و تخریبی خود را به انجام می رسانند.

شیوه عمومی عملکرد کرم ها نصب یک در پشتی (Backdoor) روی سیستم آلوده می باشد. از طریق این در پشتی سیستم آلوده تحت اختیار این بدافزار قرار می گیرد و می تواند به روش های متفاوت به رشد خود ادامه دهد. به عنوان مثال می توانند به لیست ایمیل دوستان در Address

Book دسترسی پیدا کند و از ایمیل قربانی برای ارسال ایمیل هایی حاوی بدافزارها استفاده نماید.

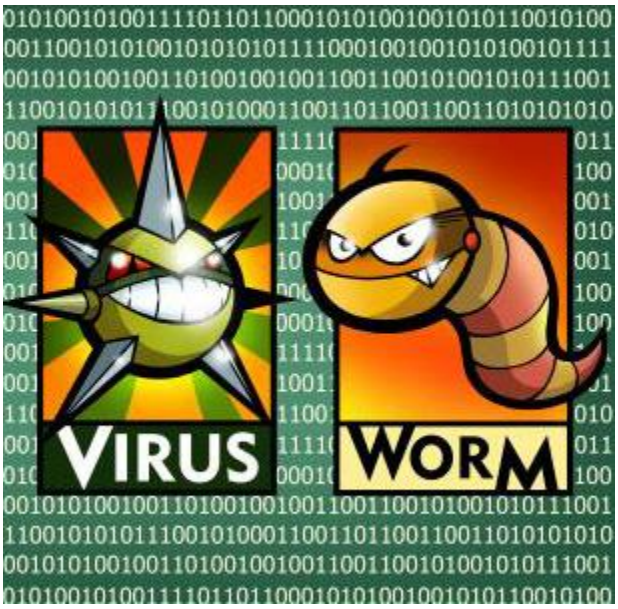
کرم ها در یک مسیر از شبکه شروع به رشد و تخریب می نمایند و به همین دلیل نیز به این نام معروف شده اند. کرم ها یکی از شایع ترین انواع بدافزار ها هستند که به اشتباه به عنوان ویروس از سوی کاربران شناخته می شوند.



کرم موریس (به انگلیسی: Morris worm) اولین کرم رایانه‌ای بود که در دوم نوامبر ۱۹۸۸ در اینترنت پخش شد.

یک مثال دیگر کرم ILOVEYOU یکی از کرم های معروفی است که توانیست از طریق ایمیل شیوع فراوانی پیدا نماید و خسارتهای بسیار سنگینی را به بار آورد.

کرم ها عمدتاً با اشغال پهنای باند به شبکه آسیب می رسانند. به عبارتی هدف کرم‌ها معمولا"استفاده از منابع می‌باشد و می‌تواند در دسترسی به منابع تاخیر ایجاد کند.



یکی از شباهتهایی که کرم ها با ویروس ها دارند و باعث شده است که گاهی اوقات این دو بدافزار با هم به اشتباه گرفته شوند نوع تکثیر آنها می باشد. کرم ها نیز مانند ویروس ها خود-همانند ساز هستند. البته در این شباهت نیز دو تفاوت نهفته است :

- کرم ها مستقل و متکی به خود هستند و برای تکثیر نیاز به کد اجرایی دیگری ندارند.
- کرم ها از طریق شبکه ها از ماشینی به ماشین دیگر منتقل می شوند.

جهت پیشگیری از آلوده شدن به این نوع بدافزارها حتماً از صحت شبکه های کامپیوتری خود اطمینان پیدا نمایید و تحت هیچ عنوان ایمیل ها ناشناخته را (حتی اگر از سوی دوستانتان ارسال شده است) باز نکنید و در صورت نیاز به دانلود فایلهای پیوست ایمیل حتماً آنها را توسط اسکنرهای امنیتی سرویس های ایمیل بررسی نمایید.

روت کیت (Rootkit) ها را دست کم نگیرید!

روت کیت ها بدافزارهایی هستند که خود و فعالیتهایشان را در کامپیوتر هدف مخفی نگه می دارند و کنترل مدیریت سیستم عامل را به دست می گیرند.

همین الان ممکن است سیستم شما به یک روت کیت آلوده باشد و خودتان از آن مطلع نباشید.روت کیت ها روز به روز قدرتمند تر و ناشناس تر می شوند و به حدی پیشرفت کرده اند که در حال حاضر در سایتهای زیرزمینی به فروش رسانده می شوند و مشتری های فراوانی از جمله دولتها و سازمان های بزرگ دارند.

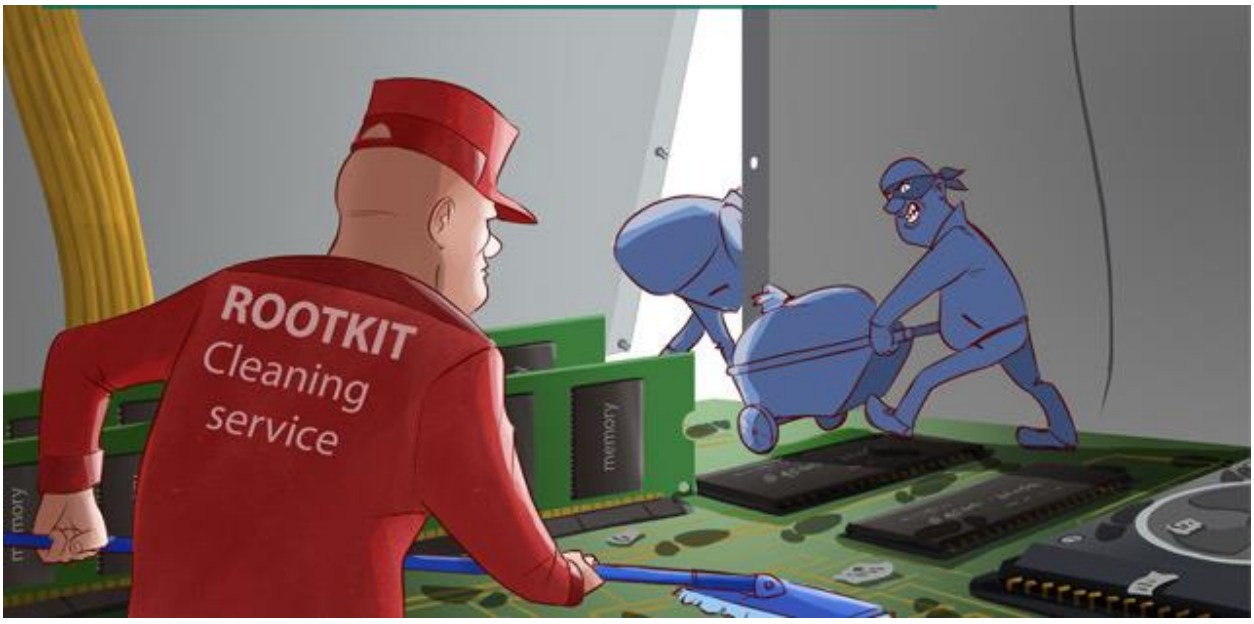
با روش مخفی سازی ایی که روت کیت ها دارند ممکن است مدت زمان زیادی سیستم عامل شما به آنها آلوده باشد بدون اینکه از آن مطلع باشید. در این مدت هکرها می توانند از منابع کامپیوتر شما استفاده کنند. بیشتر کاربران از این بابت که اطلاعات مهمی روی رایانه خود ندارند اظهار اطمینان می نمایند که لزومی ندارد مورد هجوم بدافزارها قرار بگیرند ولی این گونه نیست. حتی

اگر اطلاعات مهمی نداشته باشید کامپیوتر شما می تواند به عنوان یک واسطه (یا کارگر) برای انجام کارهای غیرقانونی هکرها مورد استفاده قرار بگیرد.

روت کیتها به منظور مخفی کردن فعالیت های سایر بدافزارها نیز بکار گرفته می شوند.

برخلاف تصور ایده ی ساخت روت کیت ها بسیار پیچیده نیست. کدهای روت کیت ها به گونه ایی در سطح های پایین کدهای سیستم عامل قرار می گیرند و به این ترتیب می توانند کلیه اعمالی که در سیستم عامل در حال وقوع است (مثل حذف کردن یک فایل یا جستجو میان فایلها) را تحت نظر بگیرند. با این ایده کلیه اعمالی که وجودشان را به خطر می اندازد را می توانند شناسایی و حذف نمایند.

البته روت کیت ها یک روش قدرتمند تر هم برای از کار انداختن آنتی ویروس ها و حفظ بقای خودشان دارند. این روش live-bait fishing نام دارد. در این روش یک فایل آلوده محافظت نشده ایجاد میکند تا آنتی ویروس آن را شناسایی کند . به هنگامی که آنتی ویروس می خواهد فایل مزبور را حذف کند روت کیت تلاش خواهد کرد تا آنتی ویروس را غیرفعال کند و از اجرای مجدد آن در آینده جلوگیری کند.



از بین بردن روت کیت ها کار ساده ایی نیست و نباید از آنتی ویروس های معمولی انتظار این کار را داشته باشید. برای شناسایی روت کیت ها لازم است از نرم افزار های امنیتی قدرتمند استفاده کنید. نرم افزارهای امنیتی بصورت دائم کل فعالیت های سیستم را بصورت چند لایه تحت نظر می کیرد و فعالیت های سطح بالای سیستم عامل را با سطح پایین مقایسه میکند و در صورتی که فعالیت مشکوک و ناهمگونی بین این لایه ها شناسایی شود بر روی آن ناحیه متمرکز شده تا روت کیت را به دام بیاندازد. نرم افزارهای امنیتی قدرتمند از فناوری پردازش ابری استفاده می کنند که این امر باعث می شود دقت و قدرت آنها بسیار بالاتر برود.

نرم افزارهای امنیتی ای که قابلیت self-protection داشته باشند نیز می توانند خود را از حملات روت کیت ها حفاظت نمایند.

موسسه هایی هستند که تست های گوناگونی جهت رتبه بندی قدرت نرم افزارهای امنیتی انجام می دهند. از این طریق می توانید نرم افزار مورد نظر خود را پیدا کنید.

حقه ی اسب‌های تروآ (Trojan horses) چگونه می تواند سیستم شما را از کار بیاندازد؟!

اسب تروآ که تروجان نیز نامیده می شود نوعی از بدافزارها هستند که توسط خود کاربر روی کامپیوتر هدف نصب می شوند چون به ظاهر هیچگونه مشکلی ندارند و برای یک کار معمولی نصب میشوند. در صورتیکه این بدافزارهای معمولاً اقدام به ایجاد یک درپشتی در سیستم عامل می کنند و راه را برای ورود هکرها باز می کنند.

لغت تروجان از افسانه ایی یونانی به نام جنگ تروجان گرفته شده است. در این افسانه یونانی‌ها اسب هایی چوبی به عنوان هدیه برای دشمن می فرستند. در حالی که درون این اسب های چوبی تعدادی سرباز قرار گرفته بودند. به محض ورود هدایا به درون قلعه سربازهای یونانی از اسب های چوبی خارج میشوند و درب قلعه را برای ورود دیگر سربازان باز میکنند.

هکرها از این طریق می توانند براحتی به سرقت اطلاعات روی کامپیوتر بپردازند و یا اینکه از کامپیوتر هدف به عنوان طعمه برای ارسال هرزنامه ها استفاده کنند.

تروجان ها برنامه هایی به ظاهر بی خطر هستند که برای رسیدن به اهدافشان باید حتماً توسط کاربر روی کامپیوتر نصب شوند. از این رو تروجان ها اغلب در قالب نرم افزارها و بازیهای کم حجم و گاهی آنلاین (که برای بازی کردن نیاز به نصب پلاگین هایی روی رایانه دارند) ارایه می شوند.

تروجان ها از این رو با ویروس ها تفاوت دارند که خود تکثیر نیستند و فقط به ایجاد راه نفوذ فکر می کنند. ابته نوعی از تروجان ها به نام تروجان مخرب نیز وجود دارند که شباهت زیادی به ویروس ها دارند چون وظیفه اصلی آنها تخریب و حذف فایل ها می باشد.

یکی از راه هایی که تروجان ها برای نفوذ به رایانه هدف استفاده می کنند باز کردن پورت 21 کامپیوتر (پورت ارسال اطلاعات) و اجازه به مهاجمان برای استفاده از FTP (پروتکل ارسال اطلاعات) می باشد.

آنتی ویروس ها اغلب قادر به شناسایی تروجان ها نیستند. البته نرم افزارهایی تحت عنوان Trojan remover وجود دارند که تروجان هایی که تا کنون شماسایی شده اند را در دیتابیس خود دارند و با بررسی سیستم شما می توانند آنها را شناسایی نمایند.

تروجانها معمولاً به وسیله دانلود نا خواسته و یا نصب بازیهای آنلاین یا برنامه‌های تحت شبکه به کامپیوتر هدف دسترسی پیدا می کنند. پس توجه داشته باشید که راه اصلی پیشگیری از آلوده

شدن به این نوع از بدافزارها نصب نکردن نرم افزارها و بازیهای اینترنتی فراوانی است که این روزها در سایتهای مختلف وجود دارند.

مقابله با جاسوس افزارها (spyware) را یاد بگیرید!

این گونه بدافزارها مستقیماً دارای اثر تخریبی نیستند ولی همانگونه که از نامشان پیداست به جاسوسی روی کامپیوتر هدف می پردازند.

البته در یک تقسیم بندی کلی می توان گفت جاسوس افزارها دو دسته هستند:

- دسته ایی از جاسوس افزارها توسط کاربر و با آگاهی کامل برای کنترل یک کامپیوتر یا شبکه ایی از کامپیوتر ها به منظور کنترل اعمال کاربران یا نیروی انسانی تحت نظرش نصب می شوند. همانند نرم افزارهایی که والدین برای کنترل کودکان نصب می کنند یا نرم افزارهی که به منظور کنترل کارمندان یک سازمان روی شبکه ایی از کامپیوترها نصب می شوند.
- دسته ایی از جاسوس افزارها بدون اجازه کاربر رایانه توسط افراد سودجو روی کامپیوتر نصب می شوند و سعی در زیر نظر گرفتن اعمال کاربر و سرقت اطلاعات مفید وی دارند.

جاسوس افزار ها بصورت پنهان به فعالیت می پردازند و بسیاری از مردم ممکن است بدون آگاهی مدت زیادی را با این جاسوس افزارها سپری کنند.

جاسوس افزارها به چند طریق ممکن است از اطلاعات شما سوء استفاده و یا مشکلاتی برای کاربری شما ایجاد کنند :

- **سرقت اطلاعات شخصی**

جاسوس افزارها می‌توانند با دست یابی به کوکی‌ها عادت‌های اینترنتی، اطلاعات کارت‌های اعتباری و بسیاری اطلاعات دیگر شما را جمع‌آوری کند همچنین با ثبت کردن کلیدهای فشرده شده توسط شما روی صفحه کلیدرمزهای عبور شما را به دست آورده و در اختیار افراد دیگر قرار دهند.

- **تاثیر منفی روی عملکرد کاربر**

ظاهر شدن مداوم پنجره‌های پاپ آپ، ایجاد نوار ابزارها و آیکون‌های جدید و ناشناخته، کاهش سرعت کامپیوتر، کاهش امنیت افراد در استفاده از اینترنت و سایر مشکلاتی که جاسوس افزار ایجاد می‌کند بر عملکرد کاربران تاثیر می‌گذارد.

- **کاهش کارایی سیستم**

همانطور که گفته شد چون جاسوس افزار نوعی برنامه‌است حافظه و پردازنده کامپیوتر را درگیر می‌کند و کارایی سیستم را به شدت کاهش می‌دهد.

- **استفاده از پهنای باند**

جاسوس افزار برای ارسال اطلاعات نیاز به برقراری ارتباط از طریق اینترنت دارد و باید از پهنای باند استفاده کند.

برای مقابله با نفوذ این بدافزارها روی کامپیوتر شما لازم است راههای نفوذ آنها را به خوبی بشناسید:

پنجره‌های پاپ آپ

پنجره‌های کوچکی که به هنگام بازدید از سایت در برابر کاربر ظاهر می‌شوند و حاوی پیام‌های مختلفی برای فریب اشخاص می‌باشند. در این پنجره‌ها اغلب دکمه‌های مختلفی مانند قبول، لغو، بستن و... وجود دارد ولی هیچ‌کدام از آنها کار اصلی خود را انجام نمی‌دهند و با فشردن هر کدام از این دکمه‌ها جاسوس افزار روی سیستم نصب می‌شود. به هیچ وجه روی محتویات پنجره های پاپ آپ کلیک نکنید و به محض باز شدن آنها را ببندید. مطمئن باشید این پنجره ها حاوی هیچ اطلاعات مفیدی برای شما نیستند.

نرم‌افزارهای ضد جاسوس افزار

بعضی نرم‌افزارهای ضدجاسوسی به جای از بین بردن جاسوس افزار آن را روی سیستم نصب می‌کنند. این مورد هم معمولاً در فضای آنلاین زیاد مشاهده می شود. سایتهایی هستند که به شما پیشنهاد اسکن آنلاین کامپیوترتان جهت از بین بردن ویروس ها می کنند. به هیچ وجه این

پیشنهاد را قبول نکنیدو از برنامه‌های مطمئن و معروف برای بالا بردن امنیت سیستم خود استفاده کنید.

برنامه‌های رایگان اینترنتی

امروزه بسیاری از کاربران اینترنت بنا بر نیاز خود برنامه‌هایی را که به صورت رایگان روی اینترنت قرار گرفته دانلود و نصب می‌کنند. اغلب صاحبان این برنامه‌ها در ازای دریافت مبلغی یا بااهداف تجاری دیگر کد جاسوس افزار را در برنامه خود قرار می‌دهند و به هنگام نصب آن نرم‌افزار جاسوس افزار نیز روی سیستم کامپیوتری قرار گرفته و شروع به کار می‌کند.

مواظب کلیدهای رنگی با عنوان Download که در غالب وبسایتهای دانلود و یا تبلیغاتی قرار دارد باشید و به هیچ وجه روی آنها کلیک نکنید. برنامه های رایگان را به هیچ وجه دانلود نکنید. تنها برنامه های رایگانی مورد اطمینان هستند که دارای وب سایت رسمی بوده و توسط مراجه نرم افزاری لایسنس های لازم را اخذ نموده اند. این انتخاب را به افرادی که در حوزه نرم افزار اطلاعات بیشتری دارند بسپارید.

دیسکت ها و فلش مموری ها

حافظه‌های جانبی قابل حمل مانند سی دی و فلش به این علت که بین سیستم‌های زیادی جا به جا می‌شوند حاوی برنامه‌های مخرب هستند.

سوء استفاده از ضعف امنیتی اینترنت اکسپلورر

اینترنت اکسپلورر نام مرورگر پیش فرضی است که روی سیستم عامل ویندوز وجود دارد. متاسفانه این مرورگر علاوه بر اشکالات کاربری ضعف های امنیتی نیز دارد.

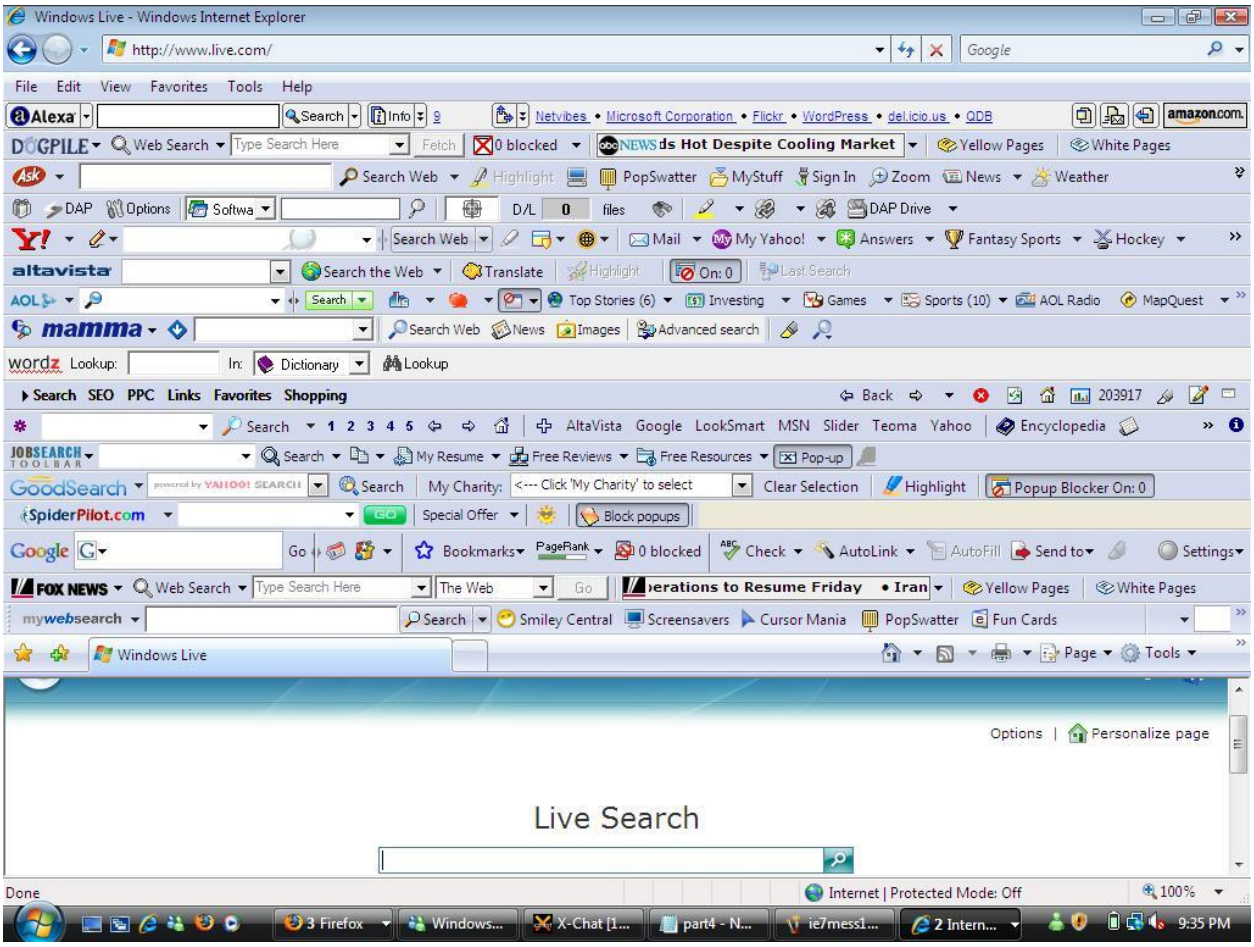
بعضی از طراحان برنامه‌های مخرب که با ضعف‌های امنیتی اینترنت اکسپلورر آشنا باشند می‌توانند در کد صفحه وب خود دستورهایی قرار دهند که به هنگام بازکردن آن صفحه با اینترنت اکسپلورر جاسوس افزار روی کامپیوتر نصب شود

ویروس‌ها

برخی ویروس‌ها حاوی کدهایی برای نصب جاسوس افزارهستند. پس اگر متوجه ویروسی روی کامپیوترتان شدید ولی به نظرتان بی آزار آمد و تغییر خاصی روی سیستم تان ایجاد نکرد فریب آن را نخورید و حتماً نسبت به پاکسازی آن اقدام نمایید.

با راه های نفوذ جاسوس افزارها آشنا شدید. علاوه بر کنترل دائمی موارد فوق به عملکرد سیستم خود نیز نظارت کافی داشته باشید تا بتوانید از وجود جاسوس افزارهای احتمالی روی آن آگاهی پیدا کنید. تشخیص آلوده بودن یک کامپیوتر به جاسوس افزار کار پیچیده ایی نیست.همانگونه که به هنگام ایجاد عیبی در اتومبیل شخصی تان از نحوه کارکرد اتومبیل به آن پی میبرید سیستم آلوده هم نشانه‌های ساده‌ای دارد که می تواند خبر از حضور یک جاسوس افزار بدهد:

- **تغییر ناگهانی صفحه خانگی مرورگر (Home Page)**: بعضی از جاسوس افزارها که برای اهداف تبلیغاتی طراحی می‌شوند بدون اجازه کاربر صفحه خانگی مرورگر اینترنتی را تغییر می‌دهند. بسیاری از افرادی که سیستم آنها آلوده شده به طور مکرر صفحه خانگی مرورگر را مطابق میل خود تنظیم نموده و با تغییر دوباره آن مواجه می‌شوند.



- **ایجاد نوار ابزارهای جدید (toolbar)** : از نشانه‌های دیگر وجود جاسوس افزار ظاهر شدن نوار ابزارهای جدید بدون خواست کاربر در پنجره مرورگر است. (توجه داشته باشید که بسیاری از تولبارها به هنگام نصب نرم افزارهای معتبر با اجازه کامل از کاربر به مرورگر افزوده می شوند و نمی توان افزوده شدن هر نوار ابزاری را نشانه ایی بر وجود جاسوس افزار دانست)

- **ظاهر شدن مداوم پنجره‌های پاپ آپ :** اگر فرد به صورت مکرر و مداوم با پنجره‌های پاپ آپ مواجه شود امکان وجود جاسوس افزار در سیستم کامپیوتری وی زیاد است.
- **تغییر آدرس توسط مرورگر:** بعضی جاسوس افزارها طوری تنظیمات مرورگر را تغییر می‌دهند که برخلاف میل کاربر و بدون توجه به آدرس وارد شده در نوار آدرس و یا نوار جستجو صفحاتی را به وی نشان دهد که در جهت اهداف تبلیغاتی طراحان آن جاسوس افزار است.
- **ایجاد آیکون‌های جدید روی صفحه نمایش :** وجود آیکون‌های جدید و ناشناخته روی صفحه نمایش بدون خواست کاربر از نشانه‌های وجود جاسوس افزار است. عدم کارایی بعضی کلیدهای صفحه کلید جاسوس افزارها کارایی کلیدهای صفحه کلید را تغییر می‌دهند به طوری که برای مثال کلید تب در پنجره مرورگر به جای جا به جایی روی پیوندها کار دیگری انجام دهد.

- **عملکرد کند کامپیوتر** : از آنجایی که جاسوس افزار یک برنامه‌است برای اجرا شدن به حافظه و پردازنده نیاز دارد و سرعت کامپیوتر را کاهش می‌دهد.

خاموش شدن دیوار آتش و ضدویروس : جاسوس افزار برای این که به راحتی اطلاعات کاربر را برای شخص ثالث ارسال کند و همچنین تنظیمات سیستم کامیوتری را تغییر دهد اغلب بدون اطلاع کاربر دیوار آتش و ضدویروس را غیر فعال می‌کند تا به اهداف خود دست یابد.

بمب های منطقی و باکتری‌ها دو بدافزار خطرناک برای رایانه شما

بمب-های منطقی (Logic Bomb) برنامه هایی هستند که به منظور ایجاد خسارت (معمولاً خسارتهای زیاد و سنگین) در زمانی خاص ایجاد می شوند. بمب های منطقی مانند ویروس ها تکثیر نمی شوند ولی می توانند از لحاظ وارد آوردن خسارت رفتاری شبیه به ویروس ها داشته باشند.

به عنوان مثال یک بمب تخریبی می تواند به محض رسیدن زمان یا وقوع شرایطی از پیش تعیین شده فعال شود و شروع به پاک نموده فایلهای روی کامپیوتر بپردازد.

بمب هیا مطقی ذاتاً مخرب هستند به همین دلیل باید تا زمان رسیدن موقعیت برای شروع فعالیتشان روی کامپیوتر هدف مخفی بمانند.

باکتری‌ها (Bacteria)

باکتری ها نوعی از بدافزارها هستند که برای فلج کردن کامپیوتر شما طراحی شده اند. همانگونه که از نام این نوع بدافزار معلوم است به شدت تکثیر پذیر است.

یکی از ویژگی های باکتری ها تغییر شکل دائم است. به این صورت که در هر بار تکثیر مادر خود را پاک میکنند و با شکل دیگری در کامپیوتر دیگری ظاهر می شوند و به این ترتیب امکان شناسایی خود را بسیار دشوار می کنند.

یکی از روش های معمول باکتری ها برای درگیر کردن منابع سیستم و در نهایت فلج کردن آن (هنگ کردن) اجرا کردن متوالی یک برنامه است. به عنوان مثال باز شدن متوالی پنجره پیغام ویندوز به صورتی که امکان بستن آن توسط کاربر وجود نداشته باشد.

باکتری ها مانند کرم ها قابلیت فعالیت در بستر شبکه را نیز دارند.

ترس افزارها (Scareware) بدافزارهایی برای اخاذی از شما!

شاید ترجمه عبارت Scareware به زورگیر معنای بهتری را برساند. ترس افزارها یا زورگیرها بدافزارهایی هستند که کاربر را با ترساندن یا تهدید کردن مجبور به انجام کاری (غالباً پرداخت مبلغی از طریق کارتهای اعتباری) می کنند.

نام دیگر این نوع بدافزارها smitfraud یا نرم افزار امنیتی فریب دهنده است. به این دلیل که زورگیرها بیشتر درقالب نرم افزارهای امنیتی یا آنتی ویروس های قلابی به نحوی اعتماد کاربر را برای نصب شدن جلب می کنند و در یک نمایش ظاهری به اسکن فایلهای روی کامپیوتر می پردازند. پس از اسکن نمایشی لیستی از بدافزارها و فایلهای مخرب را جهت ترساندن کاربر به اون نشان می دهند و با پیغامی به کاربر اعلام می نمایند که برای پاکسازی آنها باید نسخه کامل نرم افزار خریداری شود.

معمولاً در کنار این نرم افزار امنیتی یا آنتی ویروس قلابی نرم افزارهای مخرب دیگری نیز برای سرقت اطلاعات کاربر نصب می شوند.

در مواردی نیز این بدافزارها کل سیستم را مختل می نمایند و تنها راهکار پیش روی کاربر را پرداخت مبلغی به سازنده نرم افزار اعلام می کنند.

برای جلوگیری از آلوده شدن به این بدافزار زورگیر موارد زیر را رعایت کنید:

- مسدود کردن pop-up ها بر روی مرورگر
- دانلود نکردن برنامه ضد ویروس از پنجره pop-up یا لینکهای ارسالی از طریق ایمیل
- استفاده از دکمه X سیستم عامل در گوشه پنجره pop-up در هنگام بستن pop-up
- نصب برنامه ضد ویروس به همراه برنامه ضد اسپم معتبر، بروزرسانی آن و اسکن کردن دوره ای سیستم
- استفاده از آخرین نسخه سیستم عامل ها (که شامل جدیدترین بروزرسانی های امنیتی باشند) و نرم افزارهای کاربردی
- غیر فعال کردن حساب کاربری مدیر (Administrator) و استفاده از حساب کاربری استاندارد در ویندوز
- فعال نگه داشتن فایروال ویندوز یا فایروال های نصب شده روی کامپیوتر

تبلیغات مزاحم (Adware) نیز می توانند به شما آسیب برسانند!

مهمترین ابزار پیروزی در رقابت فروش تبلیغات است. تامروزه تبلیغات همه جا هستند. طبیعی است که مشاهده تبلیغات ناخواسته واقعاً آزاردهنده است. ابزارهای تبلیغاتی ناخواسته از جمله بدافزارهایی هستند که این روزها رواج بسیار زیادی یافته اند.

شیوه معمول این بدافزارها نمایش تبلیغات در قالب یک پنجره پاپ آپ یا هدایت کاربران به یک صفحه تبلیغاتی است. البته بعضی از این نرم افزارها به مرورگر وابستگی ندارند و به همراه نرم افزارهای دیگر روی کامپیوتر هدف نصب می شوند و به این راحتی ها قابل حذف نیستند.

البته این نرم افزارها عموماً خطر خاصی برای شما ندارند و صرفاً به جهت نمایش تبلیغات موجبات آزار را فراهم می آورند.ولی در بعضی موارد نیز باعث درگیر شدن منابع کامپیوتر (RAM و CPU) می شوند.

تشخیص آلوده شدن به Adware ها

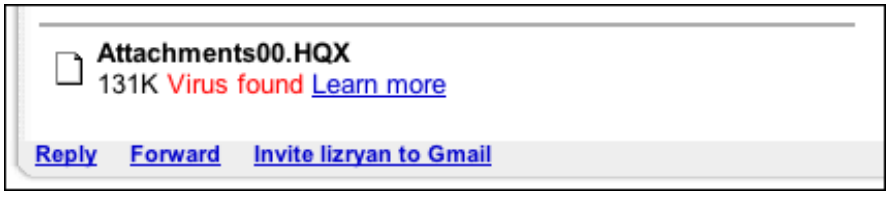
معمولاً تشخیص اینکه کامپیوتر شما به Adware آلوده شده است کار سختی نیست. بیشتر نشانه هایی که به هنگام آلوده شدن به جاسوس افزارها (spyware) مشاهده می شود برای Adware ها هم صدق می کند. به عبارتی ساده تر اغلب spyware ها برای نفوذ به رایانه هدف از ابزار Adware استفاده می کنند، پس علائمی یکسان دارند.

به عنوان مثال علائمی مانند :

- کند شدن عملکرد کامپیوتر
- تغییر Homepage مرورگر
- باز شدن پنجره های ناخواسته popup بصورت ناخواسته
- افزوده شدن تولبارهای جدید حاوی تبلیغات
- تغییر کردن موتور جستجوی پیش فرض مرورگر

پیشگیری از آلوده شدن به Adware ها

- متداول ترین روش نمایش تبلیغات ناخواسته از طریق باز شدن پنجره های pop-up در مرورگر می باشد. پس اساسی ترین اقدام در پیش گیری ، جلوگیری از باز شدن این پنجره هاست. همه مرورگرها افزونه هایی دارند که pop-up ها را غیر فعال می کند.
مرورگر گوگل کروم بصورت پیش فرض اجازه باز شدن پنجره های pop-up را نمی دهد ولی بسیاری از Adware ها از راه های دیگری نظیر کدهای جاوااسکریپت برای بازکردن این پنجره ها استفاده می کنند که برای جلوگیری از این روش هم می توانید افزونه **Javascript pop-up Blocker** استفاده کنید.
لینک دانلود از مخزن افزونه های گوگل کروم :
https://chrome.google.com/webstore/detail/javascript-popup-blocker/hiajdlfgbgnnjakkbnpdhmhfhklkbiol/related
در مرورگر فایرفاکس هم به همین روش می توانید از افزونه **Adblock-plus-pop-up** استفاده کنید:
https://addons.mozilla.org/en-US/firefox/addon/adblock-plus-/pop-up-addon



- هدف اصلی این بدافزارها پیدا کردن راهی برای دانلود فایل روی کامپیوتر شماست. پس مواظب باشید از این راه آسیب نبینید. هیچ فایلی را بدون اطمینان کامل از ایمن بودن و استاندارد بودن محتوای آن دانلود نکنید و هیچ پیغامی را نادانسته تایید نکنید. مواظب ضمیمه های ایمیل باشید و اجازه بدهید قبل از دانلود از طریق سرویس دهنده ایمیل شما اسکن شوند (البته از نتایج اسکن آنها کاملاً مطمئن نباشید)
- گاهی پیغام هایی از سمت مرورگر برای شما نمایش داده می شوند. بدون اطمینان از جعلی نبودن پیغام روی هیچ کدام از گزینه های آنها کلیک نکنید و ترجیحاً از طریق دکمه **X** آنها را ببندید. در افعال این پیغام ها گاهی شیطنت هایی می شود که معنای کلید Yes و No در آنها معکوس شود تا اگر کاربر طبق عادت برای انصراف کلید No رافشرد مجوز دانلود فایل را صادر کرده باشد.
- از یک نرم افزار امنیتی قوی که امکان Anti Adware نیز داشته باشد استفاده کنید.و بصورت دوره ایی کل سیستم خود را اسکن کنید.

آی تی پورت
درگاهی به سوی فناوری اطلاعات