آشنایی با واژه بد افزار

بدافزار (Malware) برنامه‌های رایانه‌ای هستند و به علت آن که معمولا موجب آزار کاربران یا ایجاد خسارت برای آنان می گردند، به این نام مشهور شده اند. برخی از آنان فقط برای اذیت کاربران طراحی و تولید شده اند و مثلا وی را مجبور به انجام کاری تکراری می‌کنند. اما برخی دیگر سیستم رایانه ای و داده‌های آن را مورد هدف قرار می‌دهند که ممکن است خساراتی سنگین و جبران ناپذیر به بار آورند و حتی ممکن است هدف آن سخت‌افزار سیستم کاربر باشد.

یک نرم‌افزار براساس قصد سازنده آن به عنوان یک بدافزار شناخته می‌شود و لیکن در قانون بعضا بدافزار را به عنوان یک آلودگی رایانه‌ای معرفی می کنند.

بدافزار با یک نرم‌افزار معیوب یعنی نرما فزاری قانونی ولی دارای اشکالات مضر(bug) ، تفاوت دارد. گاه بدافزار به صورت یک نرم‌افزار سالم و صحیح طراحی می‌شود و حتی ممکن است از یک سایت رسمی دانلود شود.

ویروس رایانه‌ای تنها نوعی بدافزاراست که خود را باز تولید می‌کند، اما اغلب کاربران رایانه به اشتباه به همهٔ بدافزارها ویروس می گویند.

از انواع بدافزارها می‌توان به ویروس ها، کرم ها، اسب‌های تروا، جاسوس افزارها، آگهی افزارها، روت کیت‌ها و هرزنامه‌ها اشاره کرد.

هدف از طراحی و تولید بدافزارها:

بسیاری از برنامه‌های آلوده کنندهٔ اولیه، از جمله اولین کرم اینترنتی و تعدادی از ویروس‌های سیستم عامل داس(DOS) ، به قصد آزمایش یا سرگرمی نوشته شدند. آنها عموماً به مقاصد بی‌ضرر یا فقط به قصد آزار طراحی شدند تا اینکه بخواهند خسارات جدی به سیستم‌های رایانه ای وارد کنند. در برخی موارد سازنده نمی‌توانست تشخیص دهد که چقدر کارش می‌تواند مضر باشد.

اولین سری برنامه نویسان کامپوتری وقتی دربارهٔ ویروس‌ها و ترفندهایش آموزش می دیدند، تنها به منظور تمرین یا به این قصد که ببینند ویروس چقدر شیوع پیدا می‌کند، آنها را تولید کردند. در سال ۱۹۹۹ ویروس‌های شایعی مانند ویروس ملیسا (Melissa) و ویروس دیوید (David) تنها به قصد سرگرمی نوشته شده بودند. اولین ویروس تلفن همراه در سال ۲۰۰۴ با نام ویروس کابیر (Cabir) بر روی تلفن‌های همراه منتشر شد.

با این حال مقاصد سوء به منظور خرابکاری را می‌توان در برنامه‌هایی یافت که برای ایجاد آسیب به سیستم رایانه‌ای یا از دست رفتن اطلاعات، طراحی شده‌اند. بسیاری از ویروس‌های سیستم عامل داس، با این هدف طراحی شدند تا فایل‌های موجود در یک دیسک سخت را نابود کنند یا فایل‌های سیستمی را با نوشتن اطلاعات نادرست بر روی آنها دچار اختلال کنند.

از زمان گسترش دسترسی به اینترنت پر سرعت، بدافزارهایی به منظور ایجاد سود طراحی شده‌اند. به عنوان مثال از سال ۲۰۰۳، اغلب ویروس‌ها و کرم‌های رایانه‌ای، طراحی شدند تا کنترل رایانه‌های کاربران را به منظور بهره‌گیری در بازار سیاه به کار گیرند.

بدافزارهای مسری؛ ویروس‌ها و کرم‌ها انواع بدافزارها، ویروس‌ها و کرم‌ها هستند که به خاطر نحوهٔ شیوعشان شناخته می‌شوند. عبارت ویروس کامپیوتری به برنامه‌ای اطلاق می‌شود که نرم‌افزار قابل اجرایی را آلوده کرده باشد و هنگامی که اجرا می‌شود، سبب شود که ویروس به فایل‌های قابل اجرای دیگر نیز منتقل شود. ویروس‌ها ممکن است قابلیت حمل یک بار اضافی را نیز داشته باشند، که

می‌تواند اعمال دیگر نیز انجام دهد. این اعمال اغلب خرابکارانه هستند .از سوی دیگر یک کرم برنامه‌ای است که به طور فعالانه خود را روی یک شبکه منتقل می‌کند تا رایانه‌های دیگر را نیز آلوده سازد، کرم‌ها نیز قابلیت حمل یک بار اضافی را دارند.

تعریف‌های مذکور نشان می‌دهد که تفاوت ویروس و کرم در این است که یک ویروس برای شیوع نیاز به دخالت کاربر دارد، در حالی که یک کرم خود را به طور خودکار و از طریق شبکه گسترش می دهد و در نتیجه آلودگی‌هایی که از طریق ایمیل یا فایل‌های مایکروسافت ورد (Microsoft Word) منتقل می‌شوند، ویروس شناخته می‌شوند، زیرا باید دریافت‌کنندهٔ فایل یا ایمیل آن را باز کند تا سیستم آلوده شود. برخی نویسندگان در رسانه‌های محبوب نیز متوجه این تمایز نیستند و از این عبارت‌ها به اشتباه در جای یکدیگر استفاده می‌کنند.

مخفی کارها؛ اسبهای تروا، روتکیتها و بکدورها:

اسبهای تروا :(Trojan horses) یک برنامه مخرب برای اینکه بتواند به اهدافش برسد باید قادر گردد تا اجرا شود بدون آنکه توسط کاربر یا مدیر سیستم رایانه خاموش یا پاکسازی شود. مخفی کاری همچنین این امکان را می‌دهد که بدافزار در اولین مکان نصب شود. وقتی یک برنامه خرابکار خود را به شکل چیز بی ضرر یا مطلوب درمی‌آورد، کاربران ممکن است تشویق شوند تا آن را بدون آنکه بدانند چه می‌کند، نصب کنند. این، ترفندِ اسب تروآ است.

به بیان دیگر، یک اسب تروا برنامه‌ای است که کاربر را ترغیب می‌کند تا اجرایش کند در حالی که قابلیت خرابکاریش را مخفی می‌کند. آثار منفی ممکن است بلافاصله آغاز شوند و حتی می‌توانند منجر به آثار زیانبار فراوانی گردند. از جمله حذف کردن فایل‌های کاربر یا نصب نرم افزارهای مخرب و مواردی بیشتر. اسب‌های تروا برای شروع شیوع یک کرم استفاده می‌شوند.

یکی از مرسوم ترین راه‌هایی که جاسوس افزارها تکثیر می‌شوند، از طریق یک اسب تروا است که به عنوان یک بخش از یک نرم افزار ظاهرا عادی که کاربر آنرا از اینترنت دانلود می‌کند، عمب می کند. وقتی که کاربر نرم افزار مورد نظر را نصب می‌کند، جاسوس افزار نیز در کنارش نصب خواهد شد. برای مثال اسب تروا در غالب یک نرم افزار دانلود نصب می‌شود و به صورت مستقل از نرم افزار اصلی یا مرتبط با آن شروع به دانلود برنامه و دیتای بعضا با مضمون مستهجن می نماید.

نویسندگان جاسوس افزارها سعی می‌کنند به صورت قانونی عمل نمایند و حتی ممکن است رفتار جاسوس افزار را در جملاتی مبهم در توافق نامه با کاربر قید نمایند و البته بعید است که کاربران این توافق نامه را مطالعه کنند یا متوجه منظور آن بشوند. تروها به صورت عمده و به منظور مقاصد تجاری تولید و مورد استفاده قرار می گیرند.

رد گم کن ها:

رد گم کن :(Rootkits) رد گم کن واژه مصوب فرهنگستان زبان و ادب فارسی برای (Rootkits)است. هنگامی که یک برنامهٔ خرابکار روی یک سیستم نصب می‌شود بسیار مهم است که مخفی باقی بماند تا از تشخیص و نابودی در امان باشد. همین وضعیت دربارهٔ یک مهاجم انسانی که بطور مستقیم وارد یک رایانه می‌شود برقرار است. ترفندهایی که به عنوان روتکیتها شناخته می‌شوند اجازه این مخفی کاری را می‌دهند. آن‌ها این کار را با اصلاح سیستم عامل میزبان انجام می‌دهند به نحوی که بدافزار از دید کاربر مخفی بماند. روتکیتها می‌توانند از این که یک پروسهٔ خرابکارانه در لیست پروسه‌های سیستم دیده شود ممانعت کنند، یا مانع خوانده شدن فایل‌های آن شوند. در ابتدا یک روتکیت مجموعه‌ای از ابزارها بود که توسط یک مهاجم انسانی بر روی یک سیستم یونیکس نصب می‌شد که به مهاجم اجازه می‌داد تا دسترسی مدیریتی داشته باشد. امروزه این عبارت بطور عمومی تر برای فرایندهای مخفی سازی در یک برنامهٔ خرابکار استفاده می‌شود.

بکدورها:

بکدورها :(Backdoors) یک بکدور روشی است برای خنثی سازی رویه های معمول تأیید اعتبار. وقتی یک سیستم دارای چنین رویه‌هایی باشد یک یا چند بکدور ممکن است نصب شوند تا دسترسی‌های آتی را آسان تر سازد. بکدورها ممکن است حتی پیش از یک نرم‌افزار خرابکار نصب شوند تا به مهاجمان اجازهٔ ورود دهند.

بکدورها ابزاری برای نفوذ گرها هستند که به وسیله آنها می‌توانند سیستم‌های دیگر را در کنترل خود درآورند. درهای پشتی درون شبکه، پورت‌های TCPیا UDP را باز می‌کنند و شروع به گوش کردن نموده تا دستورات نفوذگرها را اجرا کنند. درهای پشتی از جهت نداشتن قابلیت تکثیر شبیه تراواها)تروجان) هستند.

سایر بدافزارها:

جاسوس افزارها :(Spyware) بدافزارهایی هستند که بر روی رایانهٔ کاربر نصب می‌شوند و بدون اطلاع وی، اطلاعات مختلف در مورد او را جمع‌آوری می‌کنند .اکثر جاسوس‌افزارها از دید کاربرها مخفی می‌مانند و تشخیص و پیدا کردن آنها در اغلب موارد مشکل است. برخی از جاسوس‌افزارها مانند کی لاگرها ممکن است توسط مسئول یک سازمان یا شرکت بر روی رایانه ها نصب شوند تا رفتار کاربران قابل ارزیابی و بررسی باشد.

جاسوس‌افزارها هر گونه اطلاعاتی را می‌توانند جمع‌آوری کنند که این اطلاعات می‌تواند اطلاعات شخصی یک کاربرمانند انگشت و رمزهای وی بر روی اینترنت یا مشخصات حساب‌های مختلف وی مانند رمز عبور پست الکترونیکی وبانکی و غیره را شامل گردد. علاوه بر این، جاسوس افزارها می‌توانند در کنترل کامپیوتر توسط کاربر ایجاد اختلال نمایند. به عنوان مثال، جاسوس‌افزارها می‌توانند کاربر را به بازدید از یک صفحهٔ خاص اینترنتی مجبور نمایند یا برای تغییر تنظیمات رایانه او، باعث کاهش سرعت اینترنت و دسترسی غیرمجاز به رایانه شوند.

آگهی افزارها:

آگهی‌افزار یا برنامه‌های تبلیغاتی :(Adware) اینگونه برنامه‌ها همانند جاسوس‌افزارها دارای اثر تخریبی نمی‌باشند و وظیفه آنها بازکردن صفحات خاص اینترنتی جهت اهداف تجاری و تبلیغی است.

جوک‌ها:

جوک‌ها (Joke) برنامه‌هایی هستند که ادعا می‌کنند در حال انجام عملیاتی تخریبی بر روی سیستم شما می‌باشند ولی در واقع اینگونه نبوده و کار آنها چیزی جز یک شوخی ساده نمی‌باشد. متأسفانه برخی کاربران به سادگی تحت تأثیر جک‌ها قرار گرفته و با تلاش برای از بین بردن چیزی که مخرب نیست باعث ایجاد تخریب بیشتری می‌شوند.

کلک:

کلک :(Hoax) این برنامه‌ها با سوء استفاده از کم بودن اطلاعات تخصصی کاربران، آنها را فریب داده و با دستورات و توصیه‌های اشتباه باعث می‌شوند که کاربر شخصاً کاری تخریبی بر روی سیستم خود انجام دهد. به عنوان مثال وانمود می‌کنند که فایلی خاص در مسیر سیستم‌عامل یک برنامه خطرناک است و باید توسط کاربر حذف شود. غافل از اینکه این فایل سیستمی بوده و برای عملکرد درست سیستم‌عامل، وجود آن لازم است.

شماره گیرها:

شماره‌گیر :(Dialer)اینگونه برنامه‌ها وظیفه‌شان ارتباط دادن کاربر از طریق خط تلفن به سرورهایی در دیگر کشورها برای دسترسی مستقیم به اطلاعات آنها می‌باشد. این سرورها معمولاً مربوط به سایت‌های غیراخلاقی بوده و برقراری ارتباط با آنها از طریق خط تلفن باعث هزینه بسیار زیاد مالی می‌گردد.

بارگیرها:

بارگیر :(Downloader) کار اینگونه برنامه‌ها Download کردن بدافزارها و اجرای آنها است

کلیک کننده‌ها:

کلیک کننده :(Adclicker)اینگونه برنامه‌ها لینک صفحات تبلیغاتی را دنبال نموده و به این طریق حالت کلیک شدن بر روی آن صفحه تبلیغاتی خاص را شبیه سازی می‌کنند و باعث بالا رفتن hit آن می‌شوند.

سارقان رمزهای عبور:

سارقان رمزهای عبور :(Password-Stealer) اینگونه برنامه‌ها که نوعی تروجا هستند کارشان دزدی پسورد از روی سیستم‌ها و ارسال آنها برای نفوذگرها است.بهره‌کش‌هابهره‌کش‌ها (Exploits) کدهای مخربی هستند که با استفاده از آسیب‌پذیری‌های یک سیستم امکان دسترسی از راه دور به آن سیستم را فراهم می‌کنند.

کی لاگر یا کلید نگارها:

کلید نگار یا کی لاگر (Keylogger) برنامه‌هایی هستند که با قرار گرفتن در حافظه از کلیدهای زده شده توسط کاربر گزارش گرفته و در قالب یک فایل برای نفوذگر می‌فرستند. البته باید بدانیم که کی‌لاگرها به صورت سخت‌افزاری نیز وجود دارند.

برنامه‌های ضد بدافزار:

با افزایش حملات بدافزارها، توجه‌ها از محافظت در برابر ویروس‌ها و جاسوس افزارها به سمت مقابله با بد افزارها جلب شده است. در نتیجه برنامه‌های مخصوصی برای مبارزه با آنها طراحی و تولید شده اند. برنامه‌های ضد بدافزار از دو طریق با بدافزار مبارزه می‌کند:

۱ - آن‌ها محافظت بی درنگ را در برابر نصب بدافزار روی یک رایانه می‌توانند تأمین کنند، در این نوع از محافظت نرم‌افزار ضد بدافزارتمام اطلاعات ورودی از شبکه را اسکن می‌کند تا ازورود بدافزارها و تهدیدهایی که با آنها می‌آیند جلوگیری به عمل آورد. محافظت بی درنگ از بدافزار مشابه محافظت بی درنگ از ویروس عمل می‌کند. یعنی نرم‌افزار فایل‌ها را در زمان دانلود آن اسکن نموده و از فعالیت هر چیزی که بدافزار شناخته شود ممانعت به عمل می‌آورد.

۲ - برنامه‌های ضد بدافزار می‌توانند تنها به منظور تشخیص و پاکسازی بدافزارهایی که قبلاً روی یک رایانه نصب شده‌اند، مورد استفاده قرار گیرند. این نوع از محافظت در برابر بدافزار عمدتاً ساده‌تر و محبوب تر است. این نوع از ضد بدافزارها محتوای رجیستری ویندوز، فایل‌های اجرایی سیستم و برنامه‌های نصب شده روی یک رایانه را اسکن می‌کنند و لیستی از تهدیدهای پیدا شده را تهیه می‌کنند، که به کاربر اجازه می‌دهد که چه فایل‌هایی را حذف یا نگاه دارد.


GDATA
TRUST IN
GERMAN
SICHERHEIT