بخش اول

شناخت بدافزارها و روشهای مقابله با آنها

علیرضا قاضی‌سعیدی
کارشناس ارشد فناوری اطلاعات و ارتباطات

کلیدواژه‌ها: بدافزارها، ویروس، کرمها، سیستم عامل.

هدف این مقاله آشنایی خوانندگان با انواع «بدافزار»ها و روشهای برای مقابله با آنهاست. روشهای مقابله خود به دو دسته تقسیم می‌شوند: دسته اول، روشهای جلوگیری از ورود آنها به سیستم، و دستهٔ دوم، از بین بردن و یا شناسایی بدافزارهایی که سیستم را آلوده کرده‌اند.

«بدافزار»[1] به برنامه‌هایی اطلاق می‌شود که تنها هدف آنها پیاده‌سازی اهداف مهاجم است. «Malware» ترکیبی از دو لغت«Malicious» و «Software» است که در مجموع معنای بدافزار یا برنامهٔ مخرب را می‌دهد. متأسفانه بسیاری از کاربران سیستم‌های رایانه‌ای تفاوتی میان بدافزار و ویروس قائل نمی‌شوند و هر نوع آلودگی سیستم را «ویروسی شدن» می‌نامند. به همین دلیل، حتی به بسته‌های امنیتی موجود آنتی‌ویروس می‌گویند. حال آن که ویروسها تنها جزئی از خانوادهٔ بدافزار هستند وتفاوتهای بسیاری با سایر اعضای این خانواده دارند.

بدافزارها به دو دسته کلی تقسیم می‌شوند:

۱. انواعی از آنها که برای تکثیر، اجرا، انتشار و حتی ورودشان به سیستم شما، به یک برنامهٔ میزبان مثل فایلهای «Microsoft Word» نیاز دارند. از این دسته از بدافزارها می‌توان به ویروسها اشاره کرد.

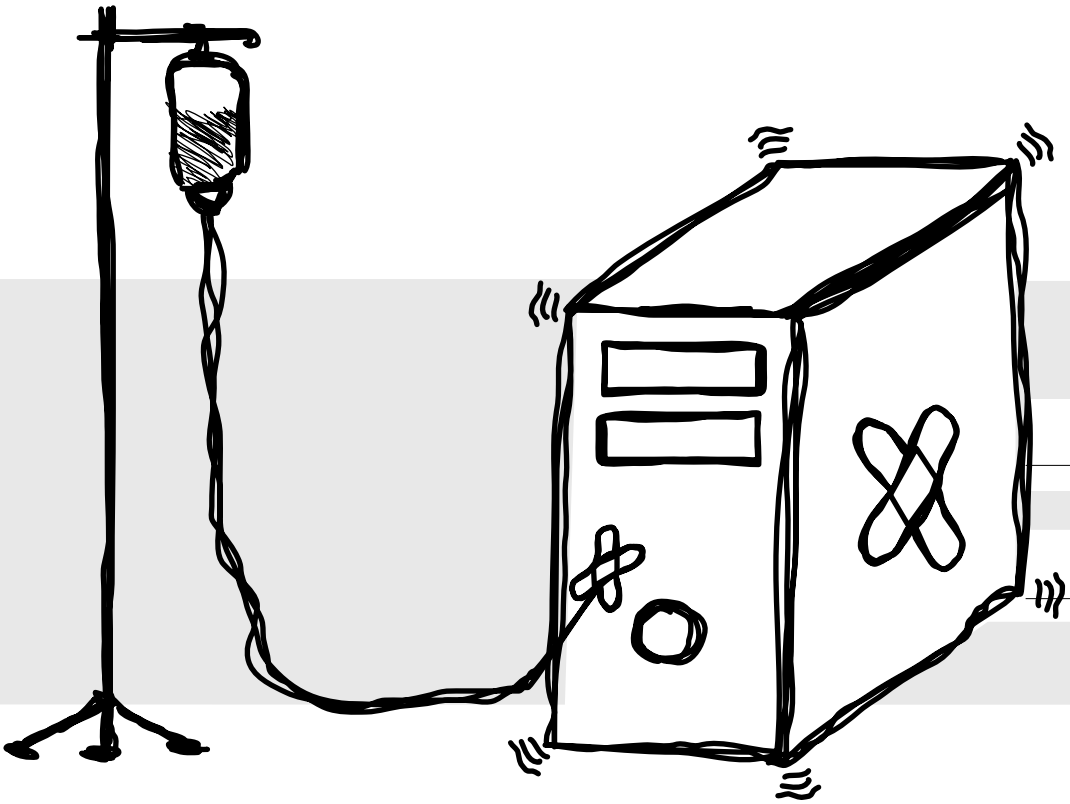
۲. انواعی از بدافزارها که مستقل هستند و به برنامهٔ میزبان نیاز ندارند. از این دسته می‌توان به «کرمها»[2] اشاره کرد.

توجه به این نکته ضروری است که هدف بدافزارها می‌تواند با هم تفاوت داشته باشد. دسته‌ای برای تخریب نرم‌افزاری، دسته‌ای برای تخریب سخت‌افزاری، گروهی برای قرار دادن منابع سیستم شما (مثل قدرت‌پردازشی cpu و حافظه) در اختیار فرد مهاجم، گروهی برای جاسوسی (برای مثال، دزدیدن حساب کاربری و رمز ورود ایمیل و یا دزدیدن شمارهٔ حساب کارتهای بانکی شما در حین تراکنش‌های مالی و ... ساخته شده‌اند.) در این بخش از مقاله ما به بررسی ویروسهای خانوادهٔ بدافزارها می‌پردازیم و در بخش‌های بعدی به بدافزارهایی هم‌چون «اسبهای تروا» (تروجان‌ها)، «کرمها» و روشهای مقابله با آنها خواهیم پرداخت.

ویروسها

همان‌طور که قبلاً نیز اشاره کردیم، ویروسها برای ورود به سیستم به میزبان نیاز دارند و به همین علت هم به این نام خوانده می‌شوند. چرا که ویروس طبیعی نیز برای ادامهٔ حیات باید در بدن یک میزبان قرار گیرد. ضمناً ویروسهای رایانه‌ای همانند ویروسهای طبیعی، هدف تکثیر شدن را دنبال می‌کنند و اصولاً برنامه‌هایی تکثیر شونده هستند.

انتشار ویروسها از طریق اجرای برنامه‌های اجرایی مثلاً با فرمت «EXE»، صورت می‌گیرد. آنها می‌توانند از طریق



«Flash disk»هـا و کارتهـای حافظـه[3] و یـا حتی هنگام «Write» کردن سـی‌دی جا به جا شوند. گاهی روش انتشار ویروسها قرارگرفتن در «Boot Sector» است. بدین مفهوم که با هر بار روشن شدن و بالا آمدن سیستم آلوده به ویروس، ویروس فعال می‌شـود و در نقاط متفاوت سیستم قرار می‌گیرد. ویروسـها حتی می‌توانند. با تغییر کدهایشان خود را به گونه‌ای تغییر دهند که شـناخته نشوند. مثلاًبا استفاده از نمادهایی خود را رمزگـذاری می‌کنند و یا حتی اطلاعات دایرکتوری دیسـک را تغییـر می‌دهند تا «بایت»های اضافه شـدهٔ ناشـی از وجود ویروس را جبران کنند.

نشانه‌های حملات ویروسی

اگـر چه نمی‌توان هر اتفاقی را به حملهٔ ویروس نسـبت داد، اما برخی از نشـانه‌هایی که می‌توانند نشانگر حضور ویروس و فعالیت آن در سیستم باشند، عبارت‌انداز:

- بوق زدن سیستم بدون نمایش رویداد خاصی؛
- گزارش برنامهٔ امنیتی سیستم مبنی بر وجود ویروس؛
- عوض شدن اسم (برچسب) درایوهای شما؛
- هنگ‌شدن دائم سیستم و مواجه شدن سیستم با خطا؛
- پایین آمدن سرعت رایانه هنگامی که برنامه‌ای را اجرا می‌کنید؛
- بالا نیامدن سیستم عامل؛
- گم شدن ناگهانی یا تغییر محتوایی فایلها و فولدرها؛
- هنگ کردن برنامهٔ مرورگر شـما مثـل «Microsoft Internet Explorer» به طور مکرر.

طبقه‌بندی ویروسها بر مبنای آن‌چه آلوده می‌کنند

- **ویروسهای بوت(Boot) یا System Sector:**

همان‌طور که از اسـم آنها مشـخص اسـت، به آلوده کردن «Boot Sector»ها می‌پردازند.

- **ویروسهای فایل:**

فایلهای اجرایی موجود در سیستم عامل را آلوده می‌کنند.

- **ویروسهای ماکرو:**

مدارک، صفحه‌های گسترده و پایگاههای اطلاعاتی، همانند «Access»، «Excel» و«Word» را آلوده می‌کنند.

- **ویروسهای شبکه:**

این ویروسـها خود را توسـط ایمیل و با استفاده از فرامین و «پروتکل»های شبکه‌ای توزیع می‌کنند.

پی‌نوشت

1. Malware
2. Worms
3. Memory Stick