دانشگاه علوم پزشکی و خدمات بهداشتی درمانی سپرجند

حراست

آشنایی با ویروس

(قسمت ششم)

تنظیم کننده :

حراست فناوری اطلاعات دانشگاه

انواع ویروسها

۱-file infecting viruses

ویروس‌ها نیز همانند هر برنامه‌ی کامپیوتری دیگر نیاز به محلی جهت ذخیره‌سازی دارند.منتهی این محل باید به گونه‌ای باشد که ویروس‌ها را به اهداف خود نزدیک و نزدیک‌تر کند.

اصولا فایل‌های موجود در یک کامپیوتر را می توان به دو گونه فایل های اجرایی و غیر اجرایی تقسیم کرد.هدف اصلی اکثر ویروس‌ها ،فایل‌های اجرایی و آلوده کردن آنهاست و کمتر ویروسی را می‌توان یافت که در یک فایل غیر اجرایی قرار گرفته و از طریق آن تکثیر شود.

این ویروس‌ها فایل‌های اجرایی(فایل هایی با پسوند . exe و com) را آلوده و همزمان با اجرای این برنامه‌ها خود را در حافظه دستگاه بار نموده و شروع به گسترش خود و آلوده کردن سایر فایل‌های اجرایی سیستم می نمایند.بعضی از نمونه‌های این ویروس‌ها، متن مورد نظر خود را به جای متن فایل اجرایی قرار می دهند.

تذکر: بعضی ازفایل‌ها را شاید نتوان ذاتا اجرایی دانست ولی چون این گونه فایل‌ها می توانند حاوی قسمت‌های اجرایی باشند لذا آنها را نوع اجرایی در نظر می گیریم.از این نوع فایل‌ها می توان به فایل‌های HTML و مستندات برنامه های Office اشاره کرد که به ترتیب ممکن است شامل اسکریپت و ماکرو باشند.اسکریپت‌ها و ماکرو ها قسمت‌های اجرایی هستند که در دل این فایل‌ها قرار گرفته و عملکرد خاصی را انجام می دهند.

۲-Macro viruses

ویروس های ماکرو,مستندات برنامه هایی را که از امکان ماکرو نویسی پشتیبانی می کنند مانند Word را آلوده می کنند.فایل‌های اینگونه برنامه‌ها اجرایی نیستند ولی درون آنها قسمت‌های اجرایی به نام ماکرو وجود دارد که می‌تواند میزبان مناسبی برای ویروس‌های کامپیوتری ماکرو باشد.

۳-Boot sector and partition table viruses

Boot sector اولین sector بر روی فلاپی و یا دیسک سخت کامپیوتر است.در این سکتور کدهای اجرایی ذخیره شده‌اند که فعالیت کامپیوتر با استفاده از آنها انجام می شود.با توجه به اینکه در

هر بار تغیر پیکر بندی کامپیوتر محتوای Boot sector مورد ارجاع قرار می گیرد,و با هر بار تغییر پیکربندی کامپیوتر محتوایboot sector هم مجدداً نوشته می شود, لذا این سکتور مکانی بسیار آسیب‌پذیر در برابر حملات ویروس‌ها می باشد.سکتور راه انداز ،واحد راه اندازی سیستم عامل است.که در سکتور شماره صفر فلاپی دیسک و یا درایوهای منطقی یک هارد دیسک قرار دارد.جدول پارتیشن بندی شامل اطلاعات تقسیم بندی هارد دیسک می‌باشد که آن نیز در سکتور شماره صفر هارد دیسک قرار دارد.این گونه ویروس‌ها با قرار گرفتن در یکی از این دو محل،هنگام راه اندازی کامپیوتر،اجرا شده و در حافظه سیستم مقیم می‌شوند و تا زمان خاموش کردن کامپیوتر یا راه اندازی دوباره،همان جا مانده و فلاپی‌ها و هارد دیسک‌های دیگر را آلوده می‌کنند. در سیتم عامل ویندوز شامل دو سری فایل است که در فرایند بوت دخالت دارند این فایل ها به طور معمول در drive ریشه یعنی c قرار دارد.

دسته اول: فایل های بوت که درsystem partition است

NTLDR-۱ Boot.ini-۲ Ntdetect.com-۳

دسته دوم: فایل های سیستم که در Boot partition است.

Ntoskernel-۱ HAL.dll-۲

فرایند boot sequence از روشن شدن تا دسترسی به منابع ادامه دارد.وقتی سیستم روشن می‌شود فرایند POST آغاز میشود. اولین مرحله load سیتم عامل را NTLDR انجام میدهد یعنی sector بوت به فایل Ntldr اشاره می کنند.

فرآیند BOOT توسط Ntldr کنترل می شود . مراحل آن عبارتند از:

Switch cpu from real mode to protected mod for 32bit addressing

این کار برای آدرس‌دهی صحیح انجام می‌شود زیرا real mode فقط تا kb۶۴۰ را آدرس دهی می‌کند.در حالی که protected mode تا gb۴ را می‌تواند آدرس دهی کند.

۴-ویروس های چندریخت(Polymorphic):

این ویروس ها در هر فایل آلوده به شکلی ظاهر می‌شوند. با توجه به اینکه از الگوریتم‌های کدگذاری استفاده کرده و ردپای خود را پاک می‌کنند، آشکارسازی و تشخیص این گونه ویروس ها دشوار است.

۵-ویروس های مخفی:این ویروس‌ها سعی می‌کنند خود را از سیستم عامل و نرم افزارهای ضدویروس مخفی نگه دارند. برای این کار ویروس در حافظه مقیم شده و حائل دسترسی به سیستم عامل می شود. در این صورت ویروس کلیه درخواست هایی که نرم افزار ضدویروس به سیستم عامل می‌دهد را دریافت می کند. به این ترتیب نرم افزارهای ضدویروس هم فریب خورده و این تصور به وجود می‌آید که هیچ ویروسی در کامپیوتر وجود ندارد. این ویروس‌ها کاربر را هم فریب داده و استفاده از حافظه را به صورت مخفیانه انجام می دهند.

۶- ویروس‌های چندبخشی

رایج ترین انواع این ویروس‌ها ترکیبی از ویروس‌های boot sector و file infecting می باشد. ترکیب انواع دیگر ویروس‌ها هم امکان پذیر است.