دانشگاه علوم پزشکی و خدمات بهداشتی درمانی سپرجند

حراست

آشنایی با ویروس

(قسمت دوم)

تنظیم کننده :

حراست فناوری اطلاعات دانشگاه

تقسیم بندی اولیه ویروسها

۱–ویروسهای مرکب(ویروس هاس چند وجهی):

از ترکیب چندین ویروس در هم ساخته شده اند و قادر خواهند بود چندین فعالیت را هم زمان انجام دهند که این امر سبب پیچیدگی کار ویروس خواهد شد.

۲–ویروس های ساده:

تک فایلی هستند و فقط یک کار انجام می دهند.

واحد تکرار کننده(replicator):وظیفه این قسمت، حصول اطمینان از بقای ویروس در سیستم است.

واحد پنهان کننده(concealer):وظیفه این قسمت مخفی سازس ویروس است.

واحد عملیات(payload):کد مخرب ویروس در این بخش قرار می گیرد.

عملکرد ویروس ها

۱-ایجاد تاخیر یا وقفه در حین عملیات سیستم اعم از اجرای برنامه ها و یا راه اندازی رایانه

۲-تخریب یا حذف برنامه ها و اطلاعات بخش های مختلف دیسک ها و یا حتی فرمت کردن دیسک ها

۳-اشغال حافظه و تکثیر در حافظه به نحوی که در حافظه جایی برای اجرای دیگر برنامه ها نمی ماند و یا باعث اختلال در کار برنامه های موجود در حافظه می شود.

۴-مجوز دسترسی به دستگاه را از طریق شبکه و بدون احراز هویت فراهم آورد.

۵-اشغال فضای دیسک

روش های آلوده سازی:

۱–بازنویسی(overwriting): ساده ترین روش آلوده سازی پاک کردن کد اصلی و جایگزین کردن کد ویروس است.کد اصلی قابل برگشت نیست و به

علت از کار افتادن کد اصلی،این ویروس به راحتی قابل تشخیص است.

۲–انگلی(parasitic):کد فایل میزبان را تغییر می دهد و به ابتدا، وسط و یا انتهای فایل میزبان متصل می شوند.البته برنامه ی میزبان تا حدودی کار می کند.اما ماهیت آن عوض شده است.

۳–همراهی(companion):فایل اصلی تغییر نمی کند یک کپی از فایل ایجاد و همراه با ویروس ر ابتدا اجرا می شود.اجرای برنامه اصلی به صورت کامل اما با کمی تاخیر است.

در قسمت بعد با خصوصیات ویروس ها و انواع برنامه های مخرب آشنا می شویم.