دانشگاه علوم پزشکی و خدمات بهداشتی درمانی سپرجند

حراست

آشنایی با ویروس

(قسمت هفتم – ضد ویروس)

تنظیم کننده :

حراست فناوری اطلاعات دانشگاه

نرم‌افزار ضدویروس چیست؟

ضدویروس اصطلاحی است که به برنامه یا مجموعه‌ای از برنامه‌ها اطلاق می‌شود که برای محافظت از رایانه‌ها در برابر ویروس‌ها استفاده می‌شود.مهم‌ترین قسمت هر برنامه ضدویروس موتور اسکن (scanning Engine) آن است.جزئیات عملکرد هر موتور متفاوت است، ولی همه‌ی آنها وظیفه شناسایی فایل‌های آلوده به ویروس را به عهده دارند و در بیشتر موارد، در صورتی که فایل آلوده باشد، ضدویروس قادر به پاکسازی و از بین بردن آن است.

انواع نرم‌افزارهای ضدویروس

دو نوع از نرم‌افزارهای آنتی ویروس عبارتند از:

نرم‌افزار **Monitoring** :نرم‌افزار نظارت، متفاوت از نرم‌افزار **scanning** است.این نرم‌افزار خسارتهای ناشی از فعالیت‌های ویروسی غیر قانونی ،مثل **overwriting** کردن فایلهای رایانه یا دوباره فرمت کردن **hard drive** رایانه را تشخیص می‌دهد و کشف می کند.

نرم‌افزار **Scanning** : این جستجوگر می‌تواند ویژگی‌های کدهای ویروس رایانه‌ای را شناسایی و در فایل‌های رایانه به جستجو کند . بیشتر نرم‌افزارهای ضدویروس، از اسکنرهای **ON-access** و **ON-demand** استفاده می کنند.

اسکنرهای **ON-demand** : در این روش این امکان به کاربر داده می شود که خودش نرم‌افزار ضدویروس را برای بررسی کردن دیسک یا یک فایل به کمک بگیرد.برای این که فعالیت فوق بازده بهتری داشته باشد، باید ضدویروس را طوری تنظیم کرد که در دوره‌های زمانی معین اقدام به اسکن کند.

ویژگی‌های یک نرم‌افزار ضدویروس مناسب

همانطور که برای هر محصولی (چه نرم‌افزاری و چه سخت‌افزاری)، آزمون‌هایی وجود دارد که کیفیت و شایستگی آن را تعیین می کند، چنین سنجش‌هایی برای یک نرم‌افزار ضدویروس هم وجود دارد.یکی از آزمون‌ها با نام آزمون **DURCH** شناخته می شود که نام آن،از حروف ابتدایی

بخش‌های پنجگانه این آزمون تشکیل شده‌اند.بنابر آزمون ،durch یک نرم‌افزار ضدویروس مناسب باید بتواند به نیازهای زیر پاسخ دهد:

۱-تست**demand**: باید بتواند هنگامی که می‌خواهید به یک فایل ، صفحه اینترنتی یا mail دسترسی داشته باشید،آنرا کنترل کند.

۲-تست **Update** : به این معنی که آنتی‌ویروس باید بتواند در بازه‌های زمانی مشخص بانک اطلاعاتی خود، که شامل الگوهای (signatures) ویروسها است را بروز کند.

۳-تست **Respond**: اینکه نرم‌افزار آنتی‌ویروس بتواند تمامی رفتارهای منطقی در برخورد با یک ویروس را از خود نشان دهد.فایل کثیف را دوباره‌سازی و تمیز کند و یا آنرا حذف نماید.

۴-تست **Check** :باید بتواند تمام فایلها از نوع مختلف را، که میتوانند محلی برای پنهان شدن ویروس باشند را کنترل کند.

۵-تست **Heuristics** :به این معنی که نرم‌افزار آنتی‌ویروس شما باید با وجود نداشتن الگوی همه ویروسها، بتواند تشخیص خطر دهد و به شما هشدار دهد که "با وجود آنکه مطمئن نیستم اما احتمالاً مسئله مشکوکی در کامپیوتر شما وجود دارد."این کنترل نیاز به آن دارد که نرم افزار آنتی‌ویروس از هوش بالایی برخورداد باشد.

روش های ویروس ها برای مقابله با آنتی ویروس ها

۱-اجتناب از آلوده کردن فایل های مشکوک : ضدویروس‌ها مرتباً جامعیت فایل‌های خود را چک می‌کنند و فایل‌های کوچک، به منظور شناسایی ویروس‌ها، نمونه برداری از ویروس با حجم کم و مطالعه‌ی رفتار ویروس به کار می برند بنابراین یک ویروس باهوش،فایل‌های مشکوک را آلوده نمی‌کند.

۲-اعمال پنهان کارانه: شامل

الف)استفاده از تکنیک‌های فشرده‌سازی یا استفاده از فضای خالی ما بین کد اصلی،برای ثابت ماندن طول فایل

ب)تغییر زمان آخرین دسترسی به فایل آلوده

ج)پایان دادن به عملیات ضد ویروس

د)دستکاری روال های ورودی/خروجی به منظور سالم جلوه دادن فایل آلوده، در پاسخ به درخواست‌های آنتی ویروس

۳-خود تغییری (**self modification**) :
ویروس‌های باهوش،درهربار آلوده‌سازی،امضای خود را تغییر می دهند.

۴-رمزنگاری با کلید متغیر:از روشهای رمزنگاری برای رمز کردن کد خود استفاده می‌کنند.یعنی هربار بعد از آلوده سازی با یک کلید جدید خود را رمز می‌کنند.

۵-کدهای چند ریختی(**polymorphism**): اولین روشی که تهدیدی جدی برای ضدویروس‌ها به شمار می آید.زیرا الگوریتم رمز نیز در هربار اجرا تغییر می‌کند.هیچ دوکدی از این ویروس‌ها با هم یکسان نیستند و تشخیص بسیار مشکل است.

در قسمت هشت با روش‌های تشخیص ویروس در آنتی ویروس آشنا می‌شویم.