تعریف ویروس:

ویروس ها یک برنامه یا یک کد(اسکریپت)بسیار کوچکی هستند که بر روی برنامه های بزرگتر سوار می شند.یعنی در بین کدهای اصلی یا فایل های اصلی یک برنامه دیگر که معمولا پر کاربرد می باشد قرار میگیرند و به محض نصب برنامه اصلی خود را وارد سیستم رایانه ای شخصی قربانی می کنند و هنگام اجرای برنامه به طور خودکار اجرا می شوند و شروع به تخریب(کارهایی که نویسنده خواسته)میکنند.

بعضی برنامه های ویروس برای تخریب عملکرد سیستم های صنعتی نوشته میشوند.

ویروس های کامپیوتری برنامه هایی هستند که پس از وارد شدن به کامپیوتر اقدامات غیر منتظره ای را انجام می دهند.با وجودی که همه ویروس ها خطرناک نیستند،ولی بسیاری از آنها با هدف تخریب انواع مشخصی از فایل ها ،برنامه های کاربردی و یا سیستم های عامل نوشته شده اند.

ویروس‌ها یک برنامه کامپیوتری است و 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 ویروس ها ،فایل های اجرایی و آلوده کردن آنهاست و کمتر ویروسی را می توان 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 فایل های اجرایی سیستم می نمایند.بعضی از نمونه‌های این ویروس‌ها، متن مورد نظر خود را به جای متن فایل اجرایی قرار می دهند.

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.

یک کاربر کامپیوتر با روشن کردن کامپیوترش از طریق کپی یک نرم افزار به داخل کامپیوترش یا از طریق اینترنت یا شبکه کامپیوتر باعث ورود نرم افزار ویروس به داخل کامپیوتر خودش میشود پس از ورود ویروس

به کامپیوتر در حافظه مقیم شده و حائل دسترسی به سیستم عامل می شود. در این صورت ویـروس کلیـه درخواست ها حتی درخواستهای نرم افزارهای ضدویروس را کنترل میکنند

اولین sector بر روی فلاپی و یا دیسک سخت کامپیوتر Boot sector است.در این سـکتور کـدهای اجرایـی ذخیره شده‌اند که فعالیت کامپیوتر با استفاده از آنها انجام می شود.با توجه به اینکه در هـر بـار تغیـر پیکـر بندی کامپیوتر محتوای Boot sector مورد ارجاع قرار مـی گیـرد,و بـا هـر بـار تغییـر پیکربنـدی کـامپیوتر محتوایboot sector هم مجدداً نوشته می شود, لذا این سکتور مکانی بسیار آسـیب‌پـذیر در برابـر حمـلات ویروس‌ها می باشدویروسهایی میتوانند فایلهای های بوت که در system partition است و فایل های سیستم که در Boot partition است را آلوده کنند

خصوصیات ویروس:

۱- برنامه نرم افزاری کوچک و مضری است که روی نوعی وسیله ذخیره ی اطلاعات کـامپیوتری قـرار مـی گسرد.
۲- بصورت خودکار و بدون دخالت اشخاص اجرا می شود.
۳- معمولا مقیم در حافظه هستند و با اجرای فایل های آلوده به ویروس در حافظه کپی می شوند.
۴- نام ویروس ها در فهرست فایل ها ظاهر نمی شود.
۵- ویروسها می توانند خود را در سایر کامپیوترها از طریق برنامه های آلوده کپی کرده و تولید مثل نمایند.
۶- ویروس های کامپیوتری توسط برنامه نویسان تکامل پیدا می کنند یعنی در حال حاضـرل تکامـل آنهـا وابسته به دخالت برنامه نویسان است.
۷- قسمت های مختلف یک ویروس به هم وابسته اند و با پاک کردن یک یا همه دستورات ویروس از بـین می رود.
۸- ویروس ها معمولا تغییرات مختلف در کامپیوتر را تشخیص داده و می توانند در مقابل آنها عکس العمل نشان دهند.

انواع برنامه های مخرب

۱- worm
۲- Trojan horse
۳- Bomb

۴- Spyware
۵- Hoax
۶- Back door

۱- worm:

کرم ها برنامه هایی هستندکه مشابه ویروس ها توان تکثیر کردن خود را دارند،ولی برعکس آنها برای گسترش خود نیاز به برنامه هایی دیگر ندارند تا آنها را آلوده کرده و تحت عنوان فایل های آلوده اقدام به انتقال و آلوده کردن دستگاه های دیگر نمایند.کرم ها معمولا از نقاط آسیب پذیر برنامه های ایمیل برای توزیع سریع و وسیع خود استفاده می نمایند.

در میان انواع wormها،کرمهای مفیدی نیز طی سالیان متمادی به منظور چک کردن کارایی سیستم و...مورد استفاده قرار گرفته اند.این wormها درون شبکه حرکت کرده،اطلاعات منابع مورد استفاده و...را چک و اطلاعاتی در مورد کارکرد شبکه را اعلام می کنند.

۲- اسبهای تروا:

یا همان Trojan horse، ویروس نیستند به دلیل آنکه بر اساس تعریف ویروس قابلیت تکثیر ندارند.اما این قدرت را دارند که فایلهای سیستم را پاک کنند،در نحوه کار نرم افزار اخلال بوجود آورند و یا سیستم را از کار بیاندازند.یک اسب تروا در حقیقت یک برنامه مخرب است که خود را به شکل یک برنامه بی خطر و معمولی نمایش میدهد و به برنامه های دیگر خود را ضمیمه می کند.

۳- logic bomb:

بمب های منطقی برنامه هایی هستند که در زمان هایی از قبل تعیین شده ،مثلا یک روز خاص،اعمالی غیر منتظره انجام می دهند.این برنامه ها فایل های دیگر را آلوده نکرده و خود را گسترش نمی دهند.

۴- برنامه های جاسوسی(spyware):

این برنامه ها به طور مستقیم دارای اثرات تخریبی نمی باشند و وظیفه اصلی آنها جمع آوری اطلاعات از روی سیستم کاربر و تحت نظر قرار دادن اعمال کاربر هنگام کار با اینترنت می باشد. اطلاعات مورد نظر این برنامه ها پیدا کردن شماره کارت اعتباری،کلمه عبور شبکه،کلمه عبور ایمیل و... می باشد.

در نهایت اطلاعات جمع آوری شده طبق تنظیمات تعریف شده ی جاسوسی به مقاصد مورد نظر ارسال می شود.

۵- فریب(Hoax):

این برنامه ها با سوءاستفاده از اطلاعات اندک کاربران آنها را فریب داده و با ارائه دستورات و توصیه های اشتباه باعث می شوند که کاربر شخصا کاری تخریبی را بر روی سیستم خود انجام دهد.به عنوان مثال وانمود می کنند که در مسیر سیستم عامل فایلی خطرناک وجود دارد و باید به وسیله کاربر حذف شود غافل از اینکه این فایل یکی از فایل های مهم سیستمی بوده و ویندوز برای فعال شدن به آن نیاز دارد.

۶-درب مخفی(back door):

برنامه نویسان و طراحان برنامه،راه هایی را برای ورود به سیستم امنیتی برای خود قرار می دهند که به درب مخفی معروف است.

به طور مثال از طریق وارد کردن یک رمز عبور سری،وارد کامپیوتر شده و علاوه بر دسترسی به اطلاعات،در بعضی از مواقع به صورت دلخواه آنها را تغییر می دهند.البته برنامه نویسان حرفه ای ایجاد این درب های مخفی را حق مسلم خود می دانند ولی مشکل اینجاست که هکر ها نیز برای مقاصد خود از درب های نخفی بهره می برند.

مراحل کار ویروس ها

۱-ورود ویروس به کامپیوتر میزبان

۲-تکثیر ویروس

۳-تخریب اطلاعات

۴-الحاق به برنامه های دیگر و نفوذ به کامپیوتر های دیگر

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

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 همه ی آنها وظیفه شناسایی فایل های 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 نرم افزار 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 می خواهید 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 تکنیک های فشرده سازی 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 درخواست های 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 می کنند.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 می کند.هیچ دوکدی از این ویروس‌ها با هم یکسان نیستند و تشخیص بسیار مشکل است.