فصل یکم- ویروس ها

۱-۱ - تعریف ویروس

به برنامه‌های رایانه‌ای که به منظور تخریب ویا سوءاستفاده از ساختار یک رایانه نوشته شود،ویروس رایانه‌ای می‌گویند. ویروس رایانه‌ای عبارتی است برای یک برنامه ناخواسته مخرب که می‌تواند روی رایانه‌هامنتشرواجراگردد.

.معمولاًویروس‌هاتوسط برنامه‌نویسان برای مقاصد گوناگون نوشته می‌شوند. اهدافی چون شهرت،انتقام، ایجاد خسارت و یا اهداف اقتصادی می‌توانند باعث ایجاد انگیزه در نوشتن ویروس کامپیوتری شوند. برخی از ویروس‌ها بسیار مخرب هستند و برخی تنها جنبه تبلیغاتی دارند.

علت نامگذاری این برنامه‌ها به ویروس به دلیل شباهت نحوه فعالیت آنها با ویروس‌ها در دنیای حقیقی است. ویروس رایانه‌ای را می‌توان برنامه‌ای تعریف نمود که می‌توان خودش را با استفاده از یک میزبان تکثیر نماید. بنابراین تعریف اگر برنامه‌ای وجود داشته باشد که دارای آثار تخریبی باشد ولی امکان تکثیر نداشته باشد،نمی‌توان آن را ویروس نامید.

معمولاً کاربران کامپیوتر به ویژه آنهایی که اطلاعات تخصصی کمتری درباره کامپیوتر دارند،ویروس‌ها را برنامه‌هایی هوشمندوخطرناک می‌دانند که خود به خود اجرا و تکثیر شده و آثار تخریبی زیادی دارند که باعث از دست رفتن اطلاعات و گاه خراب شدن کامپیوتر می‌گردند در حالی که طبق آمار تنها پنج درصد ویروس‌ها دارای آثار تخریبی بوده وبقیه صرفاً تکثیر می‌شوند. بنابراین ویروس‌های رایانه‌ای از جنس برنامه‌های معمولی هستند که توسط ویروس‌نویسان نوشته شده و سپس به طور ناگهانی توسط یک فایل اجرایی و یا جا گرفتن در ناحیه سیستمی دیسک،فایل‌ها و یا کامپیوترهای دیگر را آلوده می‌کنند. در این حال پس از اجرای فایل آلوده به ویروس و یا دسترسی به یک دیسک آلوده توسط کاربر دوم، ویروس به صورت مخفی از نسخه‌ای خودش را تولید کرده و به برنامه

های دیگر می‌چسباند و به این ترتیب داستان زندگی ویروس آغاز می‌شودوهر یک از برنامه‌ها و یا دیسک‌های حاوی ویروس، پس ازانتقال به کامپیوترهای دیگر باعث تکثیر نسخه‌هایی از ویروس وآلوده شدن دیگر فایل‌ها و دیسک‌ها می‌شوند.

بنابراین پس از اندک زمانی در کامپیوترهای موجود در یک کشور و یا حتی در سراسر دنیا منتشر می‌شوند.از آنجا که ویروس‌ها به طور مخفیانه عمل می‌کنند، تا زمانی که کشف نشده وامکان پاکسازی آنها فراهم نگردیده باشد، برنامه‌های بسیاری را آلوده می‌کنند و از این رو یافتن سازنده و یا منشأ اصلی ویروس مشکل است.

ویروس‌ها هر روز در اینترنت، بیشتروبیشتر می‌شوند. ولی تعداد شرکت‌های آنتی ویروس ثابت است. پس ما باید برای حفاظت از سیستم خود دست به کار شویم. دراین سلسله مقالات سعی داریم که نحوه مقابله با ویروس‌هاوهمین طور بیوگرافی ویروس‌هاونحوه مقابله با هر ویروس را آموزش بدهیم.

از نظر مردم عادی به برنامه‌ای که در سیستم عامل اختلالات ایجاد کندویروس است ولی باید بدانید که خود ویروس‌ها بنا به کارها و امکاناتی که دارند تقسیم‌بندی می‌شوند.ویروس‌ها مثل سایر برنامه‌ها هستند.کسانیکه ویروس رامی‌نویسندهم ازهمین برنامه‌های عادی برنامه‌نویسی استفاده می‌کند.این برنامه‌ها دقیقاً مثل چاقو می‌ماند که هم می‌شود استفاده درست کرد هم نادرست.

۱-۲ - تاریخچه ورود ویروس

۱۹۴۹:

Home

برای اولین بار تئوری برنامه‌هایی که خودشان را جایگزین می‌نمایند مطرح گردید.

۱۹۸۱: ویروس‌های Apple ۱ , Apple ۲ , Apple ۳ از اولین ویروس‌هایی بودند که پا به عرصه عمومی نهادند.این ویروس‌ها توسط کمپانی Texas A & M برای جلوگیری از کپی‌های غیر مجاز بازی‌های کامپیوتری نوشته و سپس شایع شدند. این ویروس‌ها ویژه سیستم عامل Apple II بودند.

۱۹۸۳: فرد کوهن (Fred Cohen) زمانی که روی رساله دکترایش کار می‌کرد، رسماً یک ویروس کامپیوتری را چنین تعریف نمود: «یک برنامه کامپیوتری که می‌تواند روی سایر برنامه‌های کامپیوتری از طریق تغییر دادن آنها به روشی (شاید) مانند کپی کردن خودش روی آنها، تأثیر بگذارد».

۱۹۸۶: دو برادر برنامه‌نویس پاکستانی به نام‌های «بسیط» و «امجد» کد قابل اجرای موجود در بوت سکتور یک فلاپی دیسک را با خودشان (که برای آلوده نمودن فلاپی دیسک‌های ۳۶۰□□ نوشته بودند) جایگزین کردند. تمام فلاپی‌های آلوده دارای برچسب «Brain» بودند.بنابراین، این ویروس «Brain» یا «مغز پاکستانی» نام گرفت. همزمان در کشور اتریش برنامه‌نویسی به نام رالف برگر «Ralf Burger» دریافت که یک برنامه می‌تواند از طریق چسباندن خودش به انتهای یک برنامه دیگر تکثیر شود،او با استفاده از این ایده برنامه‌ای به نام Virdem نوشت که پدیده فوق را شبیه‌سازی می‌نمود. پس از آن برگر Virdem را در کنفرانسی به همه معرفی نمود. برگر همچنین کتابی درباره ویروس‌های کامپیوتری نوشت ودرآن سورس ویروس به نام Vienna را چاپ کرد که این مسأله بعداً باعث سوءاستفاده بسیاری از افراد گردید.

۱۹۸۷: یک برنامه‌نویس آلمانی ویروسی به نام Cascade نوشت.این ویروس، اولین ویروسی بود که روش رمز کردن (Encryption) را به کار می‌برد. در این روش بیشتر کد ویروس به غیر از چند بایت از آن به صورت رمز شده در می‌آید و از آن چند بایت بعداً برای رمزگشایی بقیه کد ویروس استفاده می‌شود. در این صورت تشخیص ویروس برای آنتی ویروس‌ها بسیار مشکل‌تر می‌باشد و دیگر رشته تشخیص ویروس (که در آنتی ویروس‌ها به کار می‌رود) به چند بایت محدود نمی‌شود.

بعدها برنامه‌نویسی به نام مارک واشبرن «Mark Washburn» با استفاده از این ایده و سورس ویروس Vienna اولین ویروس هزار چهره (Polymorphic) به نام «۱۲۶۰» را نوشت.

۱۹۸۸: ویروس Jerusalem منتشر شدوبه یکی از شایع‌ترین ویروس‌ها تبدیل گشت.این ویروس درروزهای جمعه‌ای که مصادف با سیزدهم هر ماه بودند فعال می‌شدوضمن آلوده نمودن فایل‌های Com , Exe، هر برنامه‌ای که در آن روز اجرا می‌شد را نیز پاک می‌نمود.

۱۹۸۹: در ماه مارچ مهم‌ترین موضوع ویروسی، خبری بود که حکایت از فعال شدن ویروسی به نام Datacrime در ماه آوریل داشت.اما پس از بررسی سورس کد ویروس معلوم شد که این ویروس در هر تاریخی پس از روز سیزدهم اکتبر فعال شده واقدام به فرمت کردن سیلندر صفر هارد دیسک می‌نماید. بدین ترتیب کاربران تمامی محتوای هارد دیسک‌شان را از دست می‌دهند. ویروس Datacrime به احتمال زیاد در کشور هلند نوشته شده بود ولی آمریکایی‌ها اسم آن را ویروس Columbus Day گذاشتندواعتقاد داشتند که توسط تروریست‌های نروژی نوشته شده است. در این سال این ویروس علیرغم سر و صدای زیادش، خسارت‌های چندانی به بار نیاورد. در این سال همچنین ویروس‌نویسان بلغاری و روسی وارد عرصه ویروس‌نویسی شدند.

۱۹۹۰: مارک واشبرن «Mark Washburn» ابتدا ویروس هزار چهره ۱۲۶۰ و سپس بر همان اساس ویروس‌های V۲P۱ , V۲P۲ V۲P٦ را نوشت وسورس کد آنها را منتشر نمود، هر چند که بعداً ویروس‌نویسان این کدها را به کار نبردند و حتی این ویروس‌ها خطر چندانی هم نداشتند ولی ایده موجود در آنها الهام‌بخش بسیاری از ویروس‌نویسان شد.

از طرف دیگر در بلغارستان ویروس‌نویس ماهری با نام مستعار Dark Avenger چند ویروس خطرناک به نام‌های Number of the Beast , Nomenklatura , ۱۸۰۰ -DarkAvernger رانوشت. ویروس‌های وی دارای دو ویژگی مهم«آلوده‌سازی سریع» و «صدمه زدن زیرکانه» بودند. Dark Avenger به صورت فعالانه‌ای از طریق آلوده نمودن برنامه‌های

Shareware وارسال آنهااقدام به پخش ویروس‌هایش نیز می‌نمود. همچنین در این سال کمپانی Symantec نیز آنتی ویروس Norton را به بازار عرضه نمود.

۱۹۹۱: سر و کله ویروس Tequila از کشور سوئیس پیدا شد. این ویروس، ویروس هزار چهره کامل‌تری بود که پا به عرصه عمومی گذاشت و بسیار شایع شد. پس از آن نوبت انتشار ویروس هزار چهره دیگری به نام Amoeba از کشور مالت رسید. تشخیص ویروس‌های هزارچهره به دلیل اینکه پس از هر بار آلوده‌سازی ظاهرشان را تغییر می‌دهند، برای اسکنرهای ویروس بسیار سخت‌تر می‌باشد.

Dark Avenger هم درانتهای این سال موتور خود تغییر دهنده «MtE» را ابداع کرد که می‌توانست چهار میلیارد شکل مختلف به خود بگیرد و با پیوند زدن آن به هر ویروسی، یک ویروس کاملاً چند شکلی پدید می‌آمد. وی سپس با استفاده از MtE ویروس‌های Dedicated , Commander Bomber را به دو سبک کاملاً متفاوت نوشت.

۱۹۹۲: تعداد ویروس‌ها به هزار و سیصد عدد رسید که در مقایسه با ماه دسامبر سال ۱۹۹۰ چهارصد و بیست درصد افزایش یافته بود. همچنین در این سال پیش‌بینی شد که خطر ناشی از انتشار ویروس «میکلآنژ» پنج میلیون کامپیوتر را تهدید به نابودی خواهد کرد، که البته این رقم در عمل به بیش از ده هزار تا نرسید. علاوه بر اینها ویروس هزار چهره جدیدی با نام Starship پا به میدان نهاد، نرم‌افزارهای تولید ویروس توسط دو ویروس‌نویس با نام‌های مستعار Nowhere Man , Dark Angel نوشته شدندودرانگلستان نیز گروه ویروس‌نویسی ARCV تأسیس شد.

۱۹۹۴-۱۹۹۳: گروه ویروس‌نویسی جدیدی به نام Tridend در کشور هلند فعالیت خود را آغاز نمود و موتور جدیدی به نام TPE را عرضه کرد، سپس اعضای آن با استفاده از انواع مختلف TPE، ویروس‌های، Girafe Cruncher، Bosnia را نوشتند. در آمریکا هم Dark Angel به کمک موتور ابداعی‌اش موسوم به DAME ویروس Trigger را نوشت.

۱۹۹۵: Concept اولین ویروس ماکرو، نوشته شد. این ویروس اسناد نرم‌افزار Microsoft Word را مورد حمله قرار می‌داد.

۱۹۹۶: در استرالیا گروهی از ویروس‌نویسان به نام VLAD اولین ویروس ویژه سیستم عامل ویندوز موسوم به Bonz و همچنین اولین ویروس سیستم عامل لینوکس موسوم به Staog را نوشتند. علاوه بر اینها اولین ویروس ماکروی نرم‌افزار Microsoft Excel به نام Laroux نیز در این سال نوشته شد.

ویروس Strange Brew، اولین ویروسی که فایل‌های جاوا را آلوده می‌کرد، نوشته شد. این ویروس با کپی کردن خودش در میان کد فایل‌های Class و عوض نمودن نقطه شروع اجرای این فایل‌ها با نقطه شروع کد ویروسی اقدام به تغییر دادن فایل‌های Class می‌نمود. همچنین Back Orifice اولین اسب تراوایی که امکان دسترسی از راه دور به سایر سیستم‌ها را در اینترنت فراهم می‌نمود، نوشته شد و کم‌کم مقدمات ظهور ویروس‌های ماکروی نرم‌افزار Microsoft Access نیز فراهم می‌گردید.

۱۹۹۹: ویروس «ملیسا» از طریق اجرا نمودن ماکرویی که در اسناد ضمیمه شده به نامه‌های الکترونیکی موجود بود، صدمه زدن به سیستم‌ها را آغاز نمود. این ویروس همچنین برای گسترش خود از دفترچه آدرس نرم‌افزار Outlook استفاده می‌کرد و ضمیمه‌های آلوده را برای ۵۰ نفر دیگر ارسال می‌نمود. ویروس «ملیسا» سریع‌تر از تمامی ویروس‌های قبلی منتشر گردید. در این سال همچنین ویروس Corner اولین ویروسی که می‌توانست فایل‌های برنامه MS Project را آلوده سازد، نیز نوشته شد. علاوه براین، نوآوری‌های دیگری هم در دنیای ویروس‌نویسان صورت گرفت که از بین آنها می‌توان به نوشته شدن ویروس Tristate که اولین ویروس ماکروی چند برنامه‌ای بود و می‌توانست فایل‌های سه برنامه از برنامه‌های مایکروسافت (ورد، اکسل و پاور پوینت) را آلوده کند و همچنین نوشته شدن کرم Bubbleboy اشاره نمود.

این کرم هم اولین کرمی بود که وقتی کاربر نامه ساده و بدون ضمیمه‌ای را در نرم‌افزار Outlook Express باز و یا آن را پری‌ویو می‌نمود، فعال می‌گردید. حتی بدون اینکه ضمیمه‌ای به همراه نامه باشد، این کرم برای اثبات یک روش جدید نوشته شده بود و بعداً ویروس Kak از این روش بهره گرفت و به صورت گسترده‌ای شایع شد.

۲۰۰۰: ویروس I Love You درست مانند ویروس «ملیسا» به وسیله نرم‌افزار Outlook در سراسر دنیا پخش گردید. اما این ویروس از نوع اسکریپت ویژوال بیسیک بود که به صورت ضمیمه نامه الکترونیکی ارسال می‌شد. ویروس I Love You فایل‌های کاربر را پاک می‌کرد و حتی به برخی از فایل‌های تصویری و موسیقی نیز رحم نمی‌کرد. علاوه بر این، ویروس اسم کاربر و رمز عبور وی را می‌دزدید و برای نویسنده‌اش می‌فرستاد.

در این سال همچنین ویروس‌های Resume (که شبیه ویروس «ملیسا» بود) و Stages (که از روش پسوند دروغین بهره می‌گرفت) نیز ظهور کردند. در ماه ژوئن این سال و در کشور اسپانیا کرم Timofonica از نوع اسکریپت ویژوال بیسیک اولین حمله به سیستم‌های مخابراتی را آغاز نمود و در ماه نوامبر نیز اولین ویروس نوشته شده به زبان PHP ظاهر شد، این ویروس که Pirus نام گرفت، خودش را به فایل‌های HTML , PHP اضافه می‌نمود.

۲۰۰۱: ویروس Anna Kournikova در پوشش تصویر ستاره تنیس، «آنا کورنیکووا» و با روش انتشاری مشابه ویروس‌های «ملیسا» و «I love You» ظاهر شد. در ماه می این سال هم ویروس Home Page به حدود ده هزار نفر از کاربران نرم‌افزار Outlook آسیب رساند. در ماه جولای و آگوست نیز کرمهای CodeRed I، Code Red II به شبکه‌های کامپیوتری حمله نمودند.

تعداد کامپیوترهای آلوده حدود هفتصد هزار دستگاه و خسارت وارده به سیستم‌ها بالغ بر دو میلیارد دلار برآورد گردید.

حادثه مهم دیگری که در این سال به وقوع پیوست، نوشته شدن ویروس Winux یا Lindose در کشور جمهوری چک توسط Benny از اعضای گروه ۲۹ بود که قابلیت آلوده‌سازی هر دو سیستم عامل ویندوز و لینوکس را با هم داشت.

در این سال همچنین ویروس LogoLogic-A و ویروس PeachyPDF-A (اولین ویروسی که برای پخش شدن از نرم‌افزار کمپانی Adobe ویژه فایل‌های PDF استفاده می‌کرد) نیز پا به عرصه حیات گذاشتند. ولی بدون شک اهمیت هیچ یک از این ویروس‌ها به اندازه کرم Nimda نبود، این کرم که در ماه سپتامبر ظاهر شد، از تکنیک‌های برتر سایر ویروس‌های مهم به صورت همزمان استفاده می‌نمود. بنابراین توانست تا بسیار سریع گسترش یابد.