به نام خداوند جان و خرد/کزین برتر اندیشه برنگذرد

کتاب الکترونیکی

ویروسهای کامپیوتری

چیستند؟

تهیه و تدوین :مرتضی حکیمی کیا -تکنسین کامپیوتر -مهندس نرم فزار

Email: Morteza_Hakimi@yahoo.com

ویروس چیست؟

ویروس های کامپیوتری برنامه هایی هستند که مشابه ویروس های بیولوژیک گسترش یافته و پس از وارد شدن به کامپیوتر اقدامات غیرمنتظره 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.

ویروس ها هم مشابه همه برنامه های دیگر از منابع سیستم مانند حافظه و فضای دیسک سخت، توان پردازنده مرکزی و سایر منابع بهره می گیرند و می توانند اعمال خطرناکی را انجام دهند به عنوان مثال فایل های روی دیسک را پاک کرده و یا کل دیسک سخت را فرمت کنند. همچنین یک ویروس می تواند مجوز دسترسی به دستگاه را از طریق شبکه و بدون احراز هویت فراهم آورد.

برای اولین بار در سال ۱۹۸۴ واژه «ویروس» در این معنا توسط فرد کوهن در متون آکادمیک مورد استفاده قرار گرفت. در این مقاله که «آزمایشاتی با ویروس های کامپیوتری» نام داشت نویسنده دسته ای خاص از برنامه ها را ویروس نامیده و این نام گذاری را به لئونارد آدلمن نسبت داده است. البته قبل از این زمان ویروس ها در متن داستان های عملی و تخیلی ظاهر شده بودند.

بد نیست بدانید،تنها در حدود پنج درصد ویروس ها، مخرب هستند.

تاریخچه‌ی ویروس های کامپیوتری

تکنولوژی های جدید هر چند که باعث بوجود آمدن سرعت پیشرفت انسانها در مسیر زندگی گردیده است ولی درون آنها نیز مشکلاتی نهفته است که اگر این مشکلات نبود این تکنولوژی ها و علوم هیچ وقت ارتقا نمی‌یافت.

تکنولوژی های جدید هر چند که باعث بوجود آمدن سرعت پیشرفت انسانها در مسیر زندگی گردیده است ولی درون آنها نیز مشکلاتی نهفته است که اگر این مشکلات نبود این تکنولوژی ها و علوم هیچ وقت ارتقا نمی یافت. یکی از این مشکلات که در علوم کامپیوتری نهفته است و به نظر می رسد هیچوقت تمامی ندارد مبحث ویروسها است که سالانه باعث خسارت های چند میلیارد دلاری برای شرکت ها و ادارات و حتی مردم عادی می شود .

برای اولین بار در سال ۱۹۸۶ بود که دو جوان پاکستانی اعلام کردند برنامه ای نوشته اند که در قسمتی از یک دیسکت قرار میگیرد و این توانایی را دارد که در حافظه کامپیوتر مقیم شود و خود را در هر دیسکتی که پس از آن در کامپیوتر بگذارند کپی کند . این قابلیت که برنامه خود را کپی می کرد، آنها را به این سمت هدایت کرد که نام برنامه خود را ویروس بگذارند . این ویروس بی خطر بود و تنها بر چسب دیسکت را عوض می کرد .

یک سال بعد ، یک برنامه نویس دیگر به نام سوبودا اعلام کرد که ویروسی در یک برنامه به نام چارلی پیدا کرده است . این ویروس باعث می شد که کامپیوتر بعد از ۸ بار بالا آمدن reset شود .

در پاییز سال ۱۹۸۶ یک دانشجوی الکترونیک دانشگاه کالیفرنیای جنوبی در پروژه دکترای خود تحقیقات بسیار جالبی انجام داده بود . شاید کسانی که در جلسه دفاع پروژه او شرکت کردند ، نمی دانستند آن چه خواهند شنید مبنای فعالیتهای ضد اخلاقی و اخلاقی فراوانی در سالهای بعد خواهد شد . دکتر فرد کوهن در پروژه دکترای خود اثبات کرده بود که نمی توان یک برنامه جامع نوشت که با نگاه به یک فایل و یا یک دیسکت با احتمال ۱۰۰ درصد بتواند تشخیص دهد که ویروسی در آن وجود دارد یا خیر؟ به عبارت دیگر ، هیچ ضد ویروسی نمی توان نوشت که صد درصد بتواند همه ویروسها را پیدا کند . او همچنین خود یک

ویروس نوشت و سرعت انتشار آن را شبیه سازی کرد و نشان داد یک ویروس چقدر سریع می تواند رشد کند و انتشار یابد.

یکی از قانونهایی که برای انتشار ویروس لازم است . این است که ویروس خیلی سریع خرابکاریهایش را آغاز نکند . علت هم واضح است . زیرا ویروس معمولا فقط قبل از خرابکاری می تواند دیسکتهای دیگر را آلوده کند و از این طریق به کامپیوترهای دیگر سرایت کند . اگر به سرعت کامپیوتر میزبان را مورد حمله قرار دهد ، کاربر متوجه می شود و احتمال سرایت کم می شود . به هم خاطر بیشتر ویروسهای موفق ! ویروسهایی بوده اند که بعد از مدتی سکوت اجرا می شدند . مثلا ویروس Lehigh به این علت که فقط پس از ۴ بار اجرا شدن به میزبان حمله می کرد نتوانست زنده بماند. هر چند ویروس مهلکی بود و می توانست تمام هارد را پاک کند . درهمان زمان ویروسی به نام سوریو (اگر از آخر بخوانید ویروس می شود) نوشته شد که فایلهای com را مورد حمله قرار می داد . سوریو ۲ فایلهای exe و سوریو ۳ به هر دونوع فایل حمله می کرد چهارمین کار نویسنده این ویروس ، که احتمالا دانشجوی دانشگاهی در بیت المقدس بود . ویروسی به نام اورشلیم بود که در سیزدهم هرماه اگر روز جمعه به تمام فایلهای com و exe حمله می کرد و آنها را پاک می کرد این ویروس به فایل اصلی سیستم عامل Dos یعنی command.com حمله نمی کرد ، چون آن روزها مردم عادت کرده بودند از ترس ویروس ، مدام این فایل را چک کنند (ویروسهای قبلی بیشتر به این فایل حمله می کردند) نتیج این شد که ویروس اورشلیم هنوز هم زنده است . به تدریج ویروس نویسی گسترش می یافت و دانشجویان و متخصصین بیشتری طعم آزار دیگران را به روشهای تکنولوژیک می چشیدند . درهمین سالها روش جدیدی برای نوشتن ویروس ابداع شد و آن نوشتن ویروس به زبان رمز بود .

فرض کنید که برنامه ویروس شامل یک رمز گشا باشد به علاوه مقدار کد رمز شده که به این راحتیها نمی شود محتویات آن را فهمید قبل از این اتفاق ویروس کشها به دنبال الگوی خاص می گشتند و به راحتی آن را پیدا می کردند ولی با استفاده از رمز نگاری کد به رمز تبدیل می شود . در این حالت نمی توان ویروس را به راحتی تشخیص داد بلکه باید اول آن را رمز گشایی کرد و این کار مشکلی است .

در سال ۱۹۸۸ اولین ویروس کشهای تجاری به بازار آمدند و به قیمت ۵ تا ۱۰ دلار به فروش رسیدند . در همین سال ، ۲ نظر متفاوت در مورد ویروسها مطرح شد . از یک طرف ، شرکتی مثل IBM سرمایه گذاری زیادی را در جهت شناسایی ویروسها و روشهای از بین بردن آنها انجام داد و از طرف دیگر ، فرد مشهوری

مثل پتر نورتن که از متخصصین قدیمی علوم کامپیوتر است ، در مصاحبه ای اعلام کرد که به وجود ویروسها شک دارد و گفت این حرف که ویروسهای کامپیوتری منتشر شده اند مثل کروکودیل در فاضلابهای نیویورک وجود دارد (یعنی احتمال وقوع این امر وجود دارد ولی همه ما می دانیم که چنین چیزی بسیار بعید است) و همچنین یک متخصص انگلیسی نبز ادعا کرد ویروسها همه ساخته و پرداخته خیال هستند .

این اظهارات باعث شد که در یک مناظره تلویزیونی با متخصصان ویروس ، برای همه واضح شود که این یک واقعیت است نه یک خیال !

همزمان با ورود ویروس کشها به بازار تعدادی ویروس تبلیغاتی هم نوشته شد که کار خاصی نمی کرد ، فقط بر روی صفحه می نوشت که این فایل ویروسی است و بزودی تمام فایلها را آلوده خواهد کرد . این برای این کار انجام می شد که مردم ویروس را باورکنند و برای خرید ویروس کش پول خرج کنند .

در سال ۱۹۸۹ ویروسهای جدیدی نوشته شد حالا دیگر متخصصین برای همدیگر بصورت پی در پی ویروس می فرستادند تا روی آن کار کنند و ضد ویروس بنویسند . در همین سال بلغارها و روسها نیز شروع به ویروس نویسی کردند .

در سپتامبر ۱۹۸۹ شرکت IBM ویروس کش خود را به همراه توضیحات کاملی برای تمام مشتریانش فرستاد و تعداد زیادی کامپیوتر برای اولین بار scan شد .

در سال ۱۹۹۰ ویروسهای رمز شده زیادی نوشته شد که به سختی پاک می شد . همچنین ویروس کشها به اشتباه ممکن بود فایلهای سالم را ویروسی اعلام کنند . همین روزها یک فرد بلغاری که هیچ وقت نامش کشف نشد ویروسی نوشت که به سرعت انتشار می یافت .

همچنین فایلهای پشتیبانی که برای روز مبادا کپی می شد را نیز ویروسی میکرد و به همراه ویروس ، برنامه ویروس را هم می فرستاد تا مردم و برنامه نویسهای عادی نیز ویروس نویسی را یاد بگیرند و با کمی تغییرات از روی آن ویروس جدیدی بسازند .

در سال ۱۹۹۰ و زمانی که مرکز تحقیقات ضد ویروس اروپا در هامبورگ افتتاح شد ۱۵۰ ویروس و کارخانه ویروس سازی بلغارستان در حال کار بود . مقدار ویروسها به سرعت در حال افزایش بود . به عنوان مثال در دسامبر ۹۱ تعداد ویروسها ۱۰۰۰ تا و در فوریه سال بعد یعنی فقط در فاصله دو ماه ۱۳۰۰ تا بود .

بزرگترین مشکل در این سالها این بود که تعداد کسانی که بتوانند یک ویروس را در عرض چند ساعت تحلیل کنند بسیار کم بود و زمان یادگیری نیز برای تبدیل یک برنامه نویس معمولی به یک متخصص ویروسی بسیار طولانی بود . دفعه اولی که یک متخصص اورشلیم را ببیند حداقل یک هفته طول می کشد تا آن را تحلیل کند و تنها پس از تحلیل صدها ویروس شاید بتواند اورشلیم را در یک ربع تحلیل کند . مشکل همین جا بود که ویروسها روز یه روز پیچیده تر می شدند و زمان لازم برای تحلیل بالا می رفت .

مشکل بعدی در اگوست همان سال به وجود آمد که یک سری نرم افزار بسیار شیک که کار کردن با آن نسبتا ساده بود ، بیرون آمد که به کاربران معمولی اجازه می داد ویروس بنویسند در عرض یک سال صدها ویروس با استفاده از این نرم افزار ساخته شد . در همین سال عده ای سعی کردند کلکسیون ویروس بفروشند . در امریکا جان بوچانان شروع به فروش کلکسیون ویروس خود به قیمت ۱۰۰ دلار کرد . او هنوز هم این کار را ادامه می دهد .

در سالهای بین ۹۰ تا ۹۵ هر سال تعداد ویروسها ۲ برابر شد . هر چند این روند در سالهای بعدی ادامه نیافت ولی در هر صورت تعداد ویروسها در هر سال زیادتر می شود . در حال حاضر دهها هزار ویروس وجود دارند .

عده ای در رویایشان یه نرم افزارهایی فکر می کنند که به قول معروف visual English باشند . یعنی یک برنامه تحت ویندوز که با واسط گرافیکی بسیار زیبا ، توصیفات مربوط به ویروس مورد نظر شما را به زبان انگلیسی بگیرد و ویروس تحویلتان دهد .

امروزه نسل جدیدی از ویروسها در دنیای کامپیوتر و ارتباطات ظهور کرده اند که به کرم (worm) معروفند و قابلیت انتشار در شبکه های کامپیوتری را به طور وسیع و در مدت زمان بسیار کمی دارند . از معروفترین این کرمها که در سال ۲۰۰۲ شیوع پیدا کرد می‌توان به کرم معروف نیمدا (Nimda) اشاره نمود .

۲۰۰۳:این سال را سال کرمهای اینترنتی نامیده اند.

موجی از حملات موفقیت آمیز (کرمهایSobig,Blaster,Slammer) به صندوق پستی کاربران در سراسر جهان هجوم آورد.

این کرمها سرورهای پست اکترونیک را مسدود کردند ومیلیارد ها دلار خسارت به با آوردند.

تعداد ویروس های شناخته شده تا به امروز بیش از۷۰ هزار مورد بوده است.

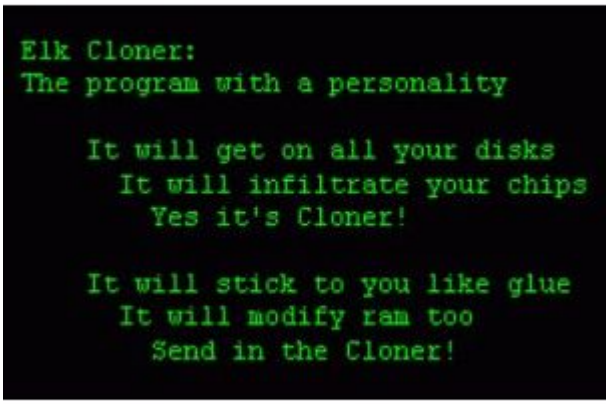
از سال ۱۹۸۱ ، هنگامی که برای اولین بار گزارش شد ویروسی کامپیوتری با سو استفاده از سهل انگاری های امنیتی شبکه، در سراسر جهان منتشر شده، تا کنون، میلیون ها نفر از کاربران کامپیوتر قربانی اسب های تروا، کرم های کامپیوتری، و ویروس ها گردیده اند.

برای مقابله با این مسئله یک صنعت کامل به نام سازندگان آنتی ویروس ها برای کمک به دفاع از توده های کاربران به وجود آمد و توسعه یافت، اما آنچه امروز مشاهده می کنیم این است که بزرگان این صنعت مانند سیمانتک هم نمی تواند با محصولات خود همیشه امنیت ۱۰۰ درصد را تضمین کنند. کد نویسان روز به روز باهوش تر شده و با تاکتیک هایی جدید تر– آسیب پذیری در فایل های مایکروسافت آفیس ، وب سایت های دولتی ، و حتی کامپیوترهای مکینتاش که مردم به غلط تصور می کردند غیرقابل نفوذند را هدف قرار داده اند. کافی است نگاهی به این تاریخ۳۰ ساله بیاندازید تا متوجه شوید جهان ویروس های رایانه ای چه دنیای بی رحمی است. در ادامه نگاهی به گذشته داریم، و لیستی ۵۰ تایی از خطرناک ترین ویروس هایی که تا کنون به رایانه های سراسر جهان آسیب می رساند را شرح داده ایم. پیام این مقاله روشن است: سهل انگاری در استفاده از فناوری خیر، حفاظت و جدی گرفتن امنیت در کار با فناوری بله. این مطلب کمک می کند تا زاویه ای جدید برای نگاه به بد افزارها داشته باشید.

Elk Cloner -۵۰

منبع احتمالی بدافزار : ایالات متحده آمریکا

سال انتشار: ۱۹۸۱



تصور می شود این ویروس اولین بدافزار منتشر شده در جهان بی رحم ویروس هاست، ویروس Elk Cloner منعکس کننده حال و هوای آغازین روزهای محاسبات رایانه ای در اوایل دهه ۸۰ بود. این بدافزار توسط نوجوانی ۱۵ ساله به نام ریچ اسکرنتا (Rich Skrenta) و با هدف تفریح و سرگرمی برای رایانه های تحت سیستم عامل «اپل دوم» و داس ۳,۳ نوشته شده و همراه با فلاپی دیسک به رایانه دوستان صاحب رایانه آلوده شده منتقل می شد. بر خلاف نسل مدرن آن، این ویروس به احتمال زیاد بیشتر کاربر را آزار می داد تا برای انتقام سیستم آلوده را نابود کند. افرادی که رایانه شان توسط «الک کلونر» آلوده شده بود در فاصله هر ۵۰ مرتبه بوت سیستم خود شعر غیر مسجع زیر را روی صفحه مشاهده کرده و صدایی می شنیدند ("It will get on all your disks / It will infiltrate your chips / Yes, it's Cloner! / It will stick to you like glue / It will modify RAM too / Send in the Cloner!") : بر روی تمام دیسکهای خود مرا پیدا می کنید / من به درون تراشه های رایانه شما نفوذ می کنم/ بله ، من کلونر هستم!/ من مانند چسب چوب به شما می چسبم / این شامل رم هم خواهد شد / کلونر را بفرستید"!

Ramen –۴۹

منبع احتمالی انتشار: نامعلوم

سال انتشار: ۱۹۹۶

یکی از موذی ترین بدافزار ها یعنی کرم Ramen جزء اولین آلوده کنندگان سیستم عامل لینوکس بود . Ramen از طریق انتشار ایمیل ها از رایانه آلوده شده به سایر رایانه ها خود را منتشر می کرد و برنامه نویسان وب را هدف قرار داده بود، که دسته ای از کاربران بودند که به احتمال زیاد بیش از سایرین از

لینوکس استفاده می کردند. کرم یک rootkit نصب می کرد، که برای مهاجم دسترسی به سیستم آلوده را فراهم می نمود. سپس تبدیل تمام فایل های تعیین شده برای کدنویسی یک صفحه وب روی سیستم آلوده را به یک پیام خصوصی تبدیل می کرد به طوری که پیام زیر در کنار تصویری از نوعی غذای محبوب نشان داده می شد) "RameN Crew Hackers looooooooooooooooove noodles." :گروه هکرهای RameNغذای نودل را دووووووووست می دارند!

Baza -۴۸

منبع احتمالی: نامعلوم

سال انتشار: ۱۹۹۵

اولین ویروسی که سیستم های ویندوز ۹۵ را آلوده کرد. همانطور که این سیستم عامل مایکروسافت پررونق شده و به طور فزاینده ای همه جا حاضر بود، به همین سرعت نیز تبدیل به هدف شماره ۱ هکرها گردید.

MacMag -۴۷

منبع احتمالی انتشار: مونترال

سال انتشار: ۱۹۸۹

اگر جنون انجام کارهای بزرگ شرط لازم برای تلاش در تغییر جهان با ویروس های کامپیوتری بوده است، هیچ جای تعجب نیست اگر یکی از اولین تروریست های سایبری مرتبط با مجلات باشد MacMag . ویروسی به سفارش ریچارد براندو، سردبیر و ناشر مجله مک ، مجله کامپیوتری مستقر در مونترال بود. ویروس به منظور آلوده کردن رایانه های مک برنامه ریزی شده بود و پیغام زیر را به طور همزمان در تمام سیستم های مک نمایش می داد: "ریچارد براندو، ناشر MacMag ، و کارکنان این مجله می خواهند از این فرصت برای انتقال پیام جهانی خود که صلح و امنیت برای تمام کاربران مکینتاش در سراسر جهان است استفاده کنند " .با این حال، متاسفانه، یک باگ در کد این ویروس وجود داشت. در عوض صلح ، بسیاری از کاربرانی که مبتلا به این الودگی شده بودند به سادگی دچار کرش و توقف سیستم خود می شدند. براندو البته هیچ گاه از کاربران خسران دیده عذرخواهی نکرد.

۴۶- Scores

منبع احتمالی انتشار: ایالات متحده آمریکا

سال انتشار: ۱۹۸۹

بعد از تحمل عذاب های ناهنجاری های محل کار مانند سختی ها و شرایط بد دستمزد، ویروس Scores کاری بود از یک کارمند ناراضی. نویسنده ناشناخته آن ویروس را طوری برنامه ریزی کرده بود که به طور خاص به دو برنامه کاربردی و نرم افزار طراحی شده توسط شرکت که او را از کار بیکار کرده بود حمله کرده و آنها را از کار بیاندازد. ویروس به تدریج از طریق سیستم ها پخش شد، و باعث آسیب عمده به برخی از نسخه های رایانه های مک می شد.

Bagle -۴۵

منبع احتمالی انتشار: آلمان

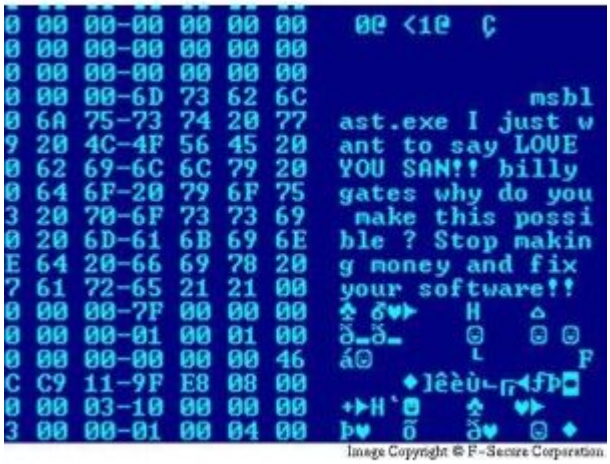
سال انتشار: ۲۰۰۴

کرم Bagle خود را از طریق ایمیل گسترش داد و تمام نسخه های ویندوز را آلوده می نمود. این کرم باعث از بین بردن ویژگی های امنیتی ، ایجاد حفره های نفوذ، از جمله درپشتی که از طریق آن مهاجم می توانست از راه دور به سیستم دسترسی داشته باشد می گردید. جالب توجه است ، کرم از حمله به تمام آدرس های ایمیل با دامنه hotmail@ یا msn@ اجتناب می نمود.

Blaster -۴۴

منبع احتمالی انتشار: چین

سال انتشار : ۲۰۰۳



ویروس Blaster تلاش گستاخانه ای برای اعتصاب و ضربه زدن به مایکروسافت و اثبات نقص های امنیتی ویندوز بود. هدف این ویروس ویندوز ایکس پی و ۲۰۰۰ و استفاده از آنها برای هماهنگ کردن حمله به Windowsupdate.comبود که به وسیله این حمله توقف و خرابی سایت مایکروسافت در نظر گرفته شده بود. در ویروس این متن جاسازی شده بود: "بیلی گیتس چرا این ایده را عملی نمی سازی؟ پول درآوردن را متوقف کن و نرم افزار خود را تعمیر کن!" ۱در همین رابطه یک جوان ۱۸ ساله از ایالت مینه سوتا برای این حمله دستگیر شد.

Download.ject -۴۳

منبع احتمالی: نامعلوم

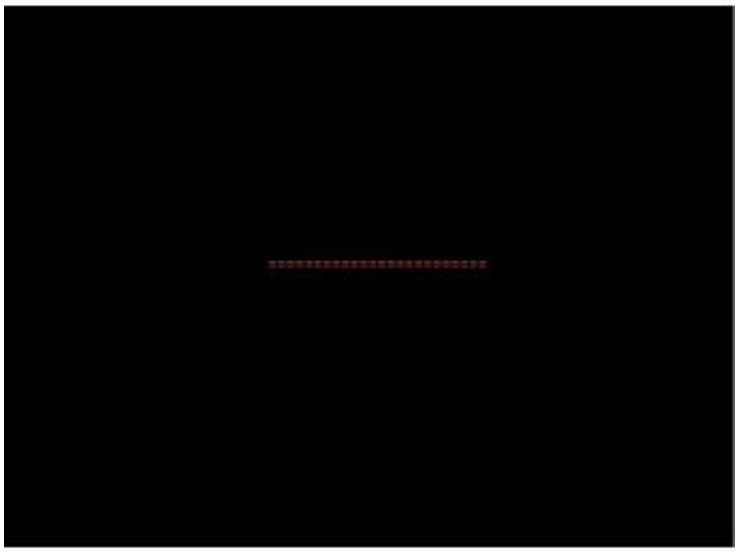
سال انتشار: ۲۰۰۴

Download.jectقطعه ای کد مخرب بود که در وب سایت شرکت ها طی یک حمله جمعی هماهنگ در ۲۳ ژوئن ۲۰۰۴ جاسازی شده بود. تصور می شود یک گروه از مجرمان سایبری سازمان یافته مسئول این حمله باشند. افرادی که از این سایت های آلوده از طریق اینترنت اکسپلورر بازدید کرده بودند نرم افزارهای مخرب روی رایانه های آنها دانلود شده بود. این اولین مورد شناخته شده بود که در آن کاربران تنها با مشاهده یک صفحه وب دچار آلودگی می گردیدند.

۴۲- Stoned

منبع احتمالی انتشار: نیوزیلند

سال انتشار: ۱۹۸۷



ویروس Stoned با یک تیر دو هدف را نشانه گرفته بود هم بیانیه ای سیاسی بود و هم اولین ویروس شناخته شده برای بوت سکتور، که بر نحوه رفتار یک کامپیوتر در استارت آپ تاثیر می گذاشت. افراد دارای رایانه آلوده به این ویروس از هر هشت بار بوت سیستم خود یک مرتبه پیام زیر را در راه اندازی مشاهده می کردند: " کامپیوتر تو در حال حاضر سنگ می شود!" هکرهای طرفدار شاه دانه از زلاند نو بر شما درود فرستاده و برنامه خود را با چند واژه امضا کرده بودند: ماری جوانا را قانونی کنید.

۴۱- Leap-A
منبع احتمالی انتشار: ایالات متحده آمریکا
سال انتشار:۲۰۰۶

ویروس جهش A -اولین ویروس کامپیوتری مدرن محسوب می شد که رایانه های مک با سیستم عامل اکس را نیز تحت تاثیر خود قرار می داد، و درست موقعی ظاهر شد که بسیاری از طرفداران استیو جابز و محصولات اپل اعتقاد داشتند این سیستم عامل نفوذ ناپذیر است. بدتر از آن این بود که ویروس از طریق برنامه محبوب iChatپخش می شد. جهش A -تلاش می کرد چهار برنامه اخیرا مورد استفاده کاربر را الوده کرده و از راه اندازی آنها جلوگیری به عمل آورد.

۴۰- Michelangelo
منبع انتشار احتمالی: نیوزیلند
سال انتشار: ۱۹۹۱

برنامه ریزی شده برای فعال سازی خود در روز تولد هنرمند رنسانس یعنی میکل آنژ (۶ مارس) ویروس Michelangeloتحت سیستمهای داس را تحت تاثیر قرار داده، و بخش های بزرگ از اطلاعات روی هارد دیسک کامپیوتر آلوده را با فایل های آلوده بازنویسی می کرد.

۳۹- Word Concept

منبع انتشار احتمالی: ایالات متحده آمریکا

سال انتشار: ۱۹۹۵

یکی از شایع ترین ویروس های دهه۱۹۹۰، Word Conceptبه عنوان اولین ماکرو ویروس شناخته می شود، که توسط نوآوری تاسف بار جاسازی در زبان برنامه های نرم افزاری شناسایی شد (اغلب ، برنامه های مایکروسافت آفیس تحت تاثیر قرار می گرفتند Word Concept .(نرم افزار همه جا حاضر مایکروسافت ورد را هدف قرار داد، و پنجه های مخرب خود را روی فایل های ورد که زمانی بی خطر بودند انداخته و آنها را آلود.

۳۸- Sadmind Worm

منبع انتشار احتمالی: چین

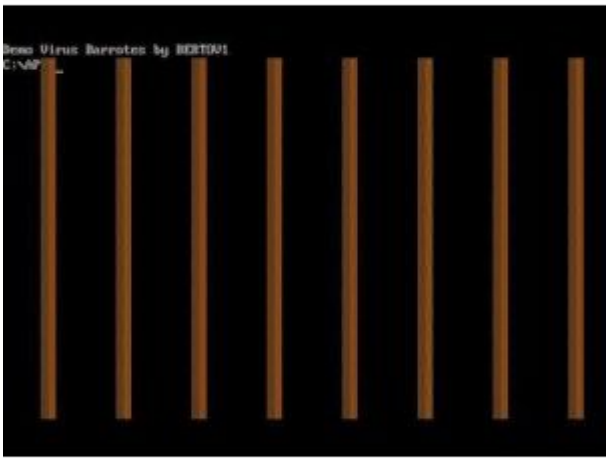
سال انتشار: ۲۰۰۱

کرم Sadmind راه خود را برای نفوذ در سیستم عامل های Sun Microsystem هموار کرده و کنترل قابلیت های مدیریتی را برای کاربر مهاجم به شکل از راه دور فعال می کرد. این کرم یکی از محبوب ترین سرورهای جهان را آلوده کرد و سبب از کار افتادن یا مخدوش شدن خدمات بیش از ۸۰۰۰ وب سایت شد.

۳۷- Barrotes Virus

منبع انتشار احتمالی: اسپانیا

سال انتشار: ۱۹۹۳



این نوع ویروس به راحتی دسترسی کاربران به هارد دیسک رایانه شان را غیر ممکن می ساخت. رایانه های آلوده یک سری میله های ضخیم مانند میله های زندان را روی صفحه نمایش نشان می دادند، که اشاره ای بی رحمانه به این واقعیت بود که اطلاعات ذخیره شده روی سیستم آلوده اسیر شده است.

Netsky –۳۶

منبع انتشار احتمالی: آلمان

سال انتشار : ۲۰۰۴

یکی از محصولات هکر آلمانی ۱۸ ساله سوئن جاشن (Sven Jaschan)به نام Netskyبه زودی به یکی از شایع ترین کرم های از طریق ایمیل گسترش یافته در جهان تبدیل شد. اعتقاد بر این است که این کرم بخشی از جنگ سایبری با نویسندگان کرم Bagle و Mydoom ، حاوی توهین در کد خود و حتی از بین بردن آنها از سیستمی که به آن ویروس ها آلوده است می باشد. در واقع این یک کرم بود که خودش بعضی کرم های دیگر را از بین می برد! همچنین صداهای آزار دهنده بیپ به صورت تصادفی در هنگام کار با سیستم آلوده شنیده می شود– که می دانید ، برای آزار دادن بیشتر کاربر است.

Laroux –۳۵

منبع انتشار احتمالی: نامعلوم

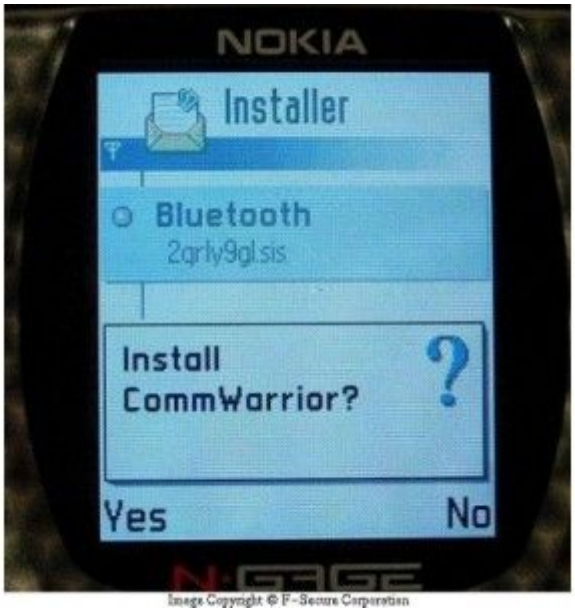
سال انتشار: ۲۰۰۲

Laroux یک ماکرو ویروس بود که باعث الودگی فایل های اکسل می شد. این هم بهانه ای دیگری بود برای به تعویق انداختن آخرین مهلت برای تحویل پروژه ها!

۳۴- Commwarrior-A

منبع احتمالی انتشار: روسیه

سال انتشار: ۲۰۰۵



اولین ویروس منتشر شده برای تلفن همراه در جهان، Commwarrior-A از طریق پیام متنی (SMS) پخش می شد و کاربران تلفن همراه را به وحشت می انداخت. در حالی که در پایان شیوع آلودگی تخمین زده

شد که تنها ۶۰ گوشی آلوده شده اند، Commwarrior-Aکافی بود تا این ترس گسترده را به کاربران القا کند که دستگاه های تلفن همراه شامل مرز جدیدی از حملات ویروس ها می شوند.

Stages –۳۳

منبع احتمالی انتشار: نامعلوم

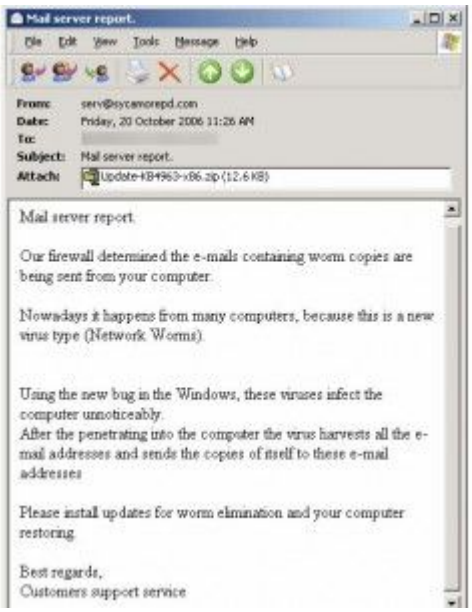
سال انتشار: ۲۰۰۰

Stagesاز طریق ایمیل پخش می شد و خود را در لباس مبدل یک شوخی در مورد مراحل زندگی از همان انواعی که شما ممکن است از دوست یا همکار خود دریافت کنید، پنهان می کرد. این ویروس در پیام متنی جعلی با فرمت txt جاسازی شده بود، که احتمال باز کردن آن را توسط کاربر زیادتر می کرد. این اولین بار ظهور این نوع ویروس ها بود.

Stration –۳۲

منبع احتمالی انتشار: نامعلوم

سال انتشار: ۱۹۹۶



کرم Stration در تاریخ کامپیوتر به جهش های بسیار سریع اش مشهور است که تا به حال بدون رقیب مانده. سرعت دگردیسی این کرم به اندازه ای بود که هر ۳۰ دقیقه یک نسخه جدید و جهش یافته از خودش ایجاد می کرد. گسترش این تغییرات، مواجهه و مقابله با آن را برای نرم افزارهای آنتی ویروس را فوق العاده دشوار می ساخت. به همین دلیل هم Stration تبدیل به قطعه ای از نرم افزارهای مخرب شد که از زمان انتشار به طور گسترده در وب توزیع شده و رایانه های بسیاری را آلوده کرد.

۳۱- Tristate

منبع احتمالی انتشار: نامعلوم

سال انتشار : ۱۹۹۹

این ماکرو ویروس، اولین ویروسی بود که قادر به آلوده کردن برنامه های مختلف بود. نام آن Tristate بود چون فایل های سه نرم افزار مهم مایکروسافت آفیس را هدف قرار می داد: ورد، اکسل و پاورپوینت. برای پایین آوردن انحصار مایکروسافت به یک سوپر ویروس نیاز بود؟ پاسخ آتش با آتش؟

۳۰- Bugbear

منبع احتمالی انتشار: نامعلوم

سال انتشار : ۲۰۰۲

کرم «لو لو» آفت بزرگی برای ائتلاف آنتی ویروس ها بود. چرا که از شیوه های گوناگونی از ایجاد آلودگی استفاده می کرد. کرم نه تنها پیچیده بود، بلکه پر از توطئه بود. ویروس کنترل کل کامپیوترهای آلوده را از مکانی دور بدست می گرفت. همچنین قادر به بازیابی رمزهاب عبور و شماره کارت اعتباری کاربران قربانی و سپس فرستادن آنها به مجموعه ای از آدرس های ایمیل از پیش تعیین شده بود Bugbear .یکی از شایع ترین ویروس های زمان خود بود، که در زمان اوج شیوع خود در هر روز ۲۲۰۰۰ کامپیوتر را در ۱۰۰ کشور جهان آلوده می کرد.

۲۹- SirCam

منبع احتمالی انتشار: ایالات متحده آمریکا

سال انتشار: ۲۰۰۱

SirCamیک مهمان ناخوانده پنهان شده در ایمیل های ناخواسته (اسپم) بود و از طریق فایل ضمیمه در اسپم ها تکثیر می گردید. این ویروس از شیوه ای غیر معمول برای آلوده کردن فایل ها استفاده می کرد. فایل های با پسوند doc یا xls را به طور تصادفی از کامپیوتر میزبان برای رسیدن به قربانی بعدی انتخاب می کرد. این کرم بسیار سریع و در محدوده وسیعی گسترش یافت و طولی نکشید که به شایع ترین کرم تا آن زمان تبدیل شد.

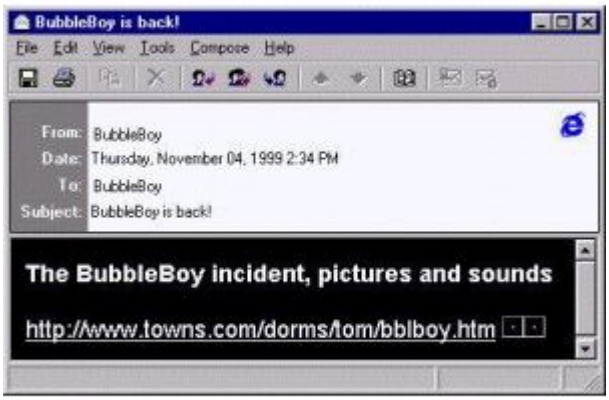
۲۸- Jerusalem

منبع احتمالی انتشار: اسرائیل

سال انتشار: ۱۹۸۷

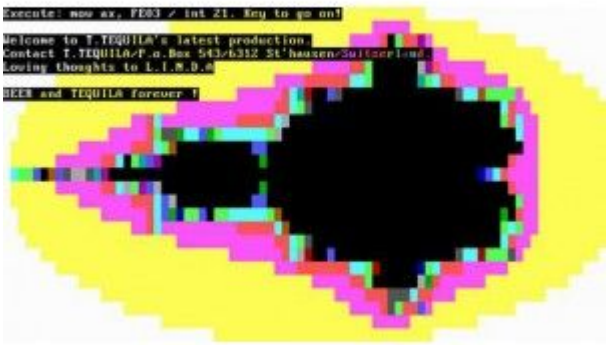
ویروسی که اولین بار در دانشگاه بیت المقدس کشف شد، ویروس Jerusalem نام داشت که از جمله اولین آلوده کننده های بین المللی بود. ویروس ماهیتی مخرب داشته و کاملا بدخیم بود، به این علت که تلاش می کرد هر فایل اجرایی بر روی سیستم میزبان را را آلوده کند. رایانه های آلوده به ویروس «اورشلیم «تا یک پنجم سرعت نرمال پردازش خود کند شده و کار با این رایانه ها فوق العاده غیر قابل تحمل می شد. از این ویروس به عنوان پیشرو در معرفی گونه ای بدنام از ویروس ها که در سال های بعد منتشر شدند و منبع آنها بلغارستان بود، از جمله Dark Avenger یاد می شود.

۲۷- Bubble Boy
منبع احتمالی انتشار: ایالات متحده آمریکا
سال انتشار: ۱۹۹۹



کاربران با شیوع این بدافزار با کابوس جدیدی مواجه شدند Bubble Boy .اولین کرم ایمیلی بود که نیازی به قرار گرفتن در پیوست ایمیل ها نداشت، صرفا مشاهده ایمیل کافی بود تا رایانه ای دچار آلودگی به این کرم گردد.

۲۶- Tequila
منبع احتمالی انتشار: نامعلوم
سال انتشار : ۱۹۹۱



Tequilaاولین ویروس چند ریختی (polymorphic) بود. ویروس ظاهر خود را هر بار که یک میزبان جدید را آلوده می کرد تغییر می داد، که شناسایی و مقابله با آن را فوق العاده دشوار نموده بود.

BadTrans –۲۵

منبع احتمالی انتشار: نامعلوم

سال انتشار : ۲۰۰۱

یکی از پررونق ترین ویروس های کامپیوتری دوران خود، کرم BadTrans یکی از نرم افزارهای مخرب ناشی از فشار اقتصادی در حال ظهور بود. کرم به طور خاص برای به دست آوردن اطلاعات مربوط به کارت اعتباری و رمزعبور طراحی شده بود، که این کار با ورود مخفیانه به سیستم، ثبت کارکرد صفحه کلید و ارسال آنها به یک ایمیل، از راه دور انجام می شد.

Solar Sunrise -۲۴

منبع احتمالی انتشار: ایالات متحده آمریکا

سال انتشار: ۱۹۹۸

بدافزار توسط دو نوجوان در کالیفرنیا ایجاد شد. ویروس Solar Sunrise با انتشار از طریق سیستم های رایانه ای که متعلق به ناسا و پنتاگون بود خبرساز شد. مدیریت بد و اتفاقاتی که در ادامه رخ داد به قدری فاجعه بار بود که گزارش به مقامات بالا و حتی به رئیس جمهور رسید. نام «طلوع آفتاب خورشیدی» اسم رمزی بود که توسط پنتاگون برای یک پروژه انتخاب شده بود. این سازمان معتقد بود که این حمله، نشانگر طلوع یک تهدید بین المللی جدید است.

Morris Internet Worm -۲۳

منبع احتمالی انتشار: ایالات متحده آمریکا

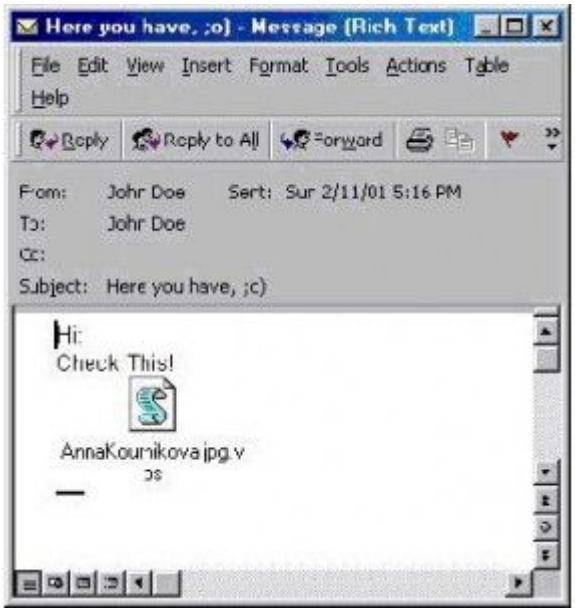
سال انتشار: ۱۹۸۸

موریس را اولین کرم تاریخ رایانه می شناسند، و برخی آن را منادی خطرات در حال تولد ناشی از اینترنت می دانند. این کرم کامپیوتر هایی را که آلوده می کرد، به طور کامل فلج می نمود. بزرگترین رایانه های قربانی مربوط به ناسا بود. موریس با آلوده کردن بی سابقه ۶۰۰۰ کامپیوتر و خسارت تخمینی ۱۰۰ میلیون دلار در زمان خود طوفانی به راه انداخت.

۲۲- Anna Kournikova

منبع انتشار احتمالی: هلند

سال انتشار : ۲۰۰۱



کرم «آنا کورنیکوا» با توجه به محبوبیت نام پرطرفدار خود، خیلی زود گسترش یافت. شیوه کار کرم به این صورت بود که نوید یک عکس از این ستاره تنیس در فایل عکس پیوست را می داد. هنگامی که ایمیل آلوده باز می شد، کرم خود را به تمام آدرس های دفترچه مخاطبین رایانه میزبان تکثیر و برای آنها نیز این ایمیل آلوده ارسال می شد. محبوبیت کرم منجر به بروز تعدادی کرم مشابه در ادامه شد، از جمله کرم های منتسب به جنیفر لوپز و بریتنی اسپیرز.

Zombie -۲۱

منبع احتمالی انتشار: چین

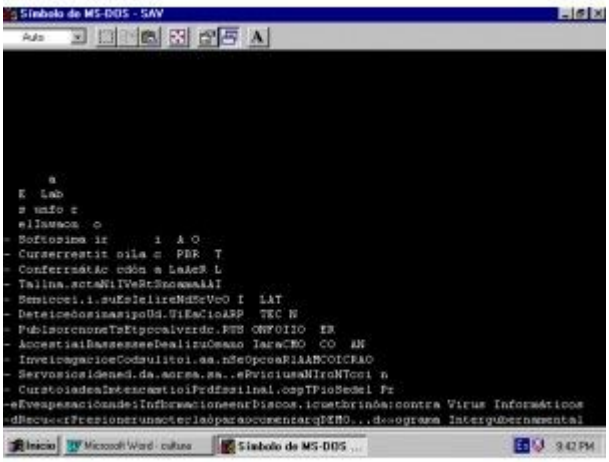
سال انتشار: ۲۰۱۰

ویروسی مخصوص تلفن همراه که وقتی یک گوشی را آلوده کرد، به طور مداوم پیام های متنی از گوشی شما می فرستد. زامبی به سرعت از زادگاه خود یعنی چین در سراسر جهان منتشر شد. جالب آنکه ویروسی که به عنوان برنامه آنتی ویروس مطرح شده بود، بنا به گزارش ها یک میلیون تلفن همراه را آلوده کرد و میلیون ها دلار خسارت به بار آورد. متون ارسالی نیز هرزنامه هایی بود که لینک هایی را به افراد دیگر معرفی می کرد که سایت های هکرها بودند و از طریق کلیک روی لینک ها برای هکرها سبب کسب درامد می شدند.

Dark Avenger -۲۰

منبع احتمالی انتشار: بلغارستان

سال انتشار: ۱۹۸۹

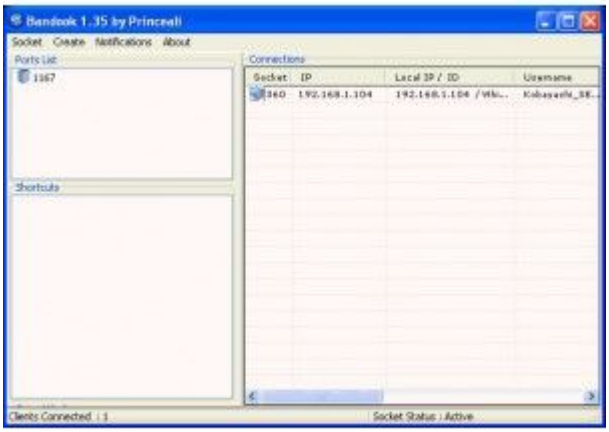


از برجسته ترین ویروس های منتشر شده از بلغارستان که در اواخر دهه ۸۰ میلادی گسترش یافت، Dark Avengerبود. این ویروس اولین ترس عمومی در رسانه های بین المللی را در میان کاربران پدید آورد. ویروس سیستم عامل های «ام اس داس» را با پر کردن کد های بی فایده انباشته و باعث کرش سیستم می شد. این ویروس شامل این پیام مرموز بود: " ادی زنده است... جایی درون زمان"

۱۹- Bandook

منبع احتمالی انتشار: نامعلوم

سال انتشار: ۲۰۰۵



Bandookیک تروجان «در پشتی» بود که ویندوز ۲۰۰۰، ایکس پی، ۲۰۰۳ و ویستا را تحت تاثیر قرار می داد. این تروجان فایروال ویندوز را دور می زد و دسترسی از راه دور مهاجم را به سیستم شما فراهم می کرد. رفتار این تروجان مشابه پسر عموی خود، Beast Trojanبود.

۱۸- Beast Trojan

منبع احتمالی انتشار: دلفی

سال انتشار: ۲۰۰۲

این کرم مبتنی بر ویندوز به شخص مهاجم کنترل کاملی بر روی کامپیوتر آلوده می داد، از جمله دسترسی به تمام فایل ها با توانایی آپلود، دانلود، اجرا یا حذف فایلها.

۱۷- Benjamin

منبع احتمالی انتشار: ایالات متحده آمریکا

سال انتشار: ۲۰۰۲

ویروس « بنجامین » کامپیوترها را از طریق برنامه به اشتراک گذاری فایل Kazaa آلوده می نمود. ویروس به عنوان آهنگی محبوب به منظور فریب کاربران برای دانلود آن معرفی می شد. هنگامی که این ویروس یک بار روی سیستم اجرا می شد، اتصال به اینترنت رایانه میزبان را مسدود و تمام ظرفیت هارد دیسک را پر می کرد.

۱۶- CIH aka Chernobyl

منبع احتمالی انتشار: تایوان

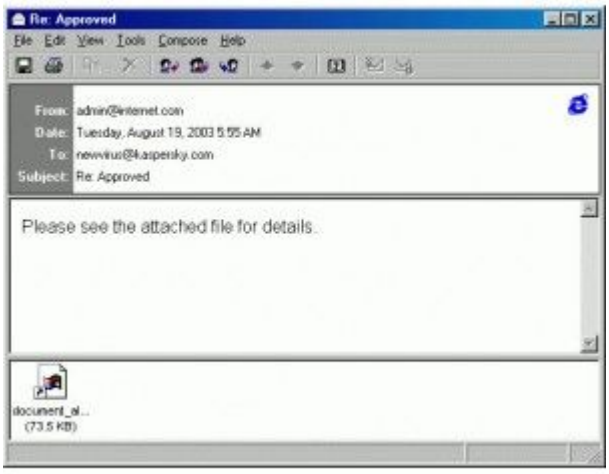
سال انتشار: ۱۹۹۸

ویروس «چرنوبیل» باعث آسیب ۸۰ میلیون دلاری به رایانه ها شد. این ویروس رایانه های مجهز به ویندوز ۹۵، ۹۸ و ME را آلوده کرده و می توانست روی فایل های هارد دیسک رونویسی کرده یا از بوت شدن سیستم جلوگیری کند. نام آن برگرفته از یک فاجعه بود: ویروس در همان روزی منتشر شد که سال ها قبل از آن انفجار راکتور هسته ای چرنوبیل در شوروی رخ داد.

۱۵- Explorer.zip
منبع احتمالی انتشار: ایالات متحده آمریکا
سال انتشار: ۱۹۹۹

این کرم به قربانیان با حذف فایل های ورد، اکسل و پاورپوینت خسارت دردآوری وارد می کرد. کرم در عین حال روش هوشمندانه ای برای گسترش خود در سراسر وب داشت Explorer.zip :در متن ایمیل ها جستجو کرده و به طور خودکار جواب دارای فایل پیوست آلوده به کرم را در پاسخ به آنها با استفاده از تیتر اصلی ارسال می کرد.

۱۵- SoBig
منبع احتمالی انتشار: ایالات متحده آمریکا
سال انتشار: ۲۰۰۳

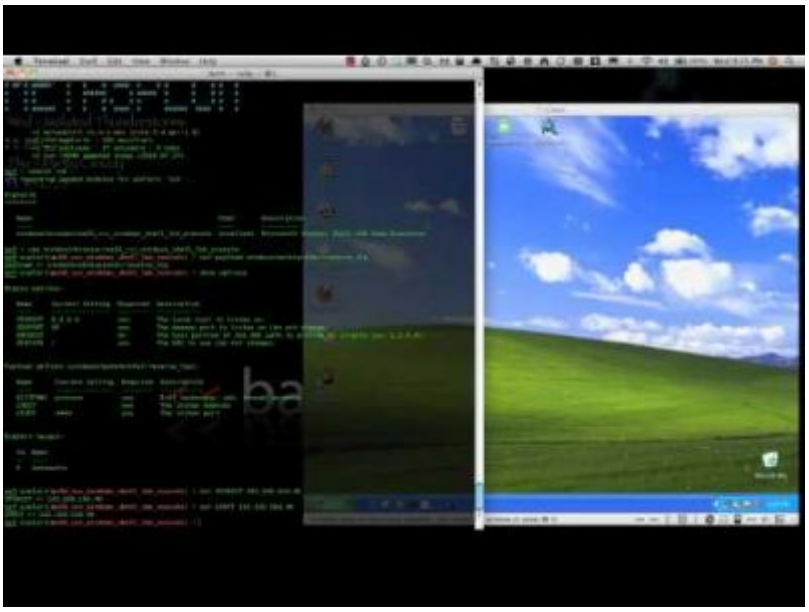


SoBigمیلیون ها کامپیوتر تحت ویندوز را آلوده کرد. این بدافزار ایمیل هایی به مخاطبین رایانه آلوده شده با عناوینی مانند "پاسخ: برنامه کاربردی درخواستی شما" و "متشکرم" ارسال شده و حاوی متنی بود که گیرنده نامه را به لینک "برای دریافت جزئیات پیوست را بازدید کنید،" هدایت می کرد، که چیزی نبود جز مواجهه با عذاب گرفتاری به بدافزار جدید. هنگامی که با SoBig آلوده می شدید، شما یک فرستنده اسپم به دوستان خود بودید.

۱۳- Stuxnet

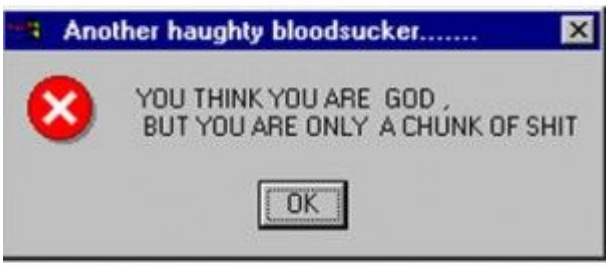
منبع احتمالی انتشار: ایران

سال انتشار: ۲۰۱۰



کرم «استاکس نت»در میان کارشناسان سبب ایجاد وحشت شد، چرا که ظاهرا توانایی از کار انداختن تاسیسات صنعتی و هسته ای را داشت. شاید بتوان آن را اولین بدافزار با قابلیت تخریب سخت افزاری خارج از کامپیوتر نامید. در همین زمینه کارشناسان امنیت سایبر در مورد یک مسابقه تسلیحاتی جدید هشدار داند. به نظر می رسد که هدف استاکس نت ایران بوده است.

۱۲- Magistr
منبع احتمالی انتشار: ایالات متحده آمریکا
سال انتشار: ۲۰۰۱



کرم Magistr قوی و مخرب بود. این کرم، فایل های ذخیره شده روی هارد دیسک های آلوده را با فایل های خود بازنویسی کرده و سبب نابودی اطلاعات به این شیوه شده و سبب کرش سیستم می گردید. همچنین Magistr در برابر آنتی ویروس ها مقاوم بود و بسیاری تلاش های معمول برای حذف آن را مسدود کرده و بی اثر می نمود.

۱۱- Sasser
منبع احتمالی انتشار: آلمان
سال انتشار: ۲۰۰۴

»ساسر» توسط سوئن جاشن ایجاد شد که شهرت خود را از برنامه نویسی ویروس Netsky که در در ادامه بدان اشاره می شود بدست آورده بود، با این تفاوت که ساسر دست پخت هکر برای انجام ماموریتی بزرگ و ویرانگر بود. چرا که برآوردها نشان می داد بر اثر این بدافزار ۱۸ میلیون دلار آسیب به صنعت رایانه وارد گردید. آلودگی سبب خساراتی منجمله خاموشی ارتباطات ماهواره ای خبرگزاری های فرانسه و لغو پروازهای Delta Airlinesشد و این تنها بخشی از اثرات ویرانگر این بدافزار بود.

۱۰- Mariposa

منبع احتمالی انتشار: اسپانیا

سال انتشار: ۲۰۱۰

این ویروس یک botnet یا شبکه ای از سیستم های آلوده شده بود که در بیش از ۱۹۰ کشور گسترش یافته و ۱۲,۷ میلیون رایانه را آلوده کرد. مقامات پلیس که موفق به شکست حلقه آلودگی شدند، اعتقاد دارند این آلودگی ها از اسپانیا نشات گرفته است و هدف آن سرقت شماره کارت اعتباری و اطلاعات بانکی قربانیان بوده است.

۹- Klez

منبع احتمالی انتشار: روسیه

سال انتشار: ۲۰۰۲

Klezرکوردی را که پیش از این در اختیار SirCam بود، شکست و تبدیل به گسترده ترین کرم تا آن زمان در تاریخ رایانه شد. رفتار کرم شبیه کرم قدیمی تر بود، یعنی بازنویسی فایل ها با فایل های آلوده که حجمشان صفر بود. علاوه بر این، Klezتلاش به غیر فعال کردن برنامه آنتی ویروس به منظور زنده نگه داشتن خود می نمود.

۸- SQL Slammer

منبع احتمالی انتشار: بریتانیا

سال انتشار: ۲۰۰۳

بدافزار SQL Slammer سرور ها را هدف قرار داده، و آنها را با قطعات کوچکی از کد که به آدرس های IP تصادفی فرستاده می شد، بمباران می کرد .سرورهای گرفتار شده با ترافیک مصنوعی یا کند شده و سرعت ارائه خدمات به کلاینت های آنها پایین می آمد، یا به کلی از ارائه سرویس ناتوان می گشتند .بخشی از قربانیان مهم شامل سرورهای بانک مرکزی امریکا، خطوط هوایی «قاره ای (Continental) «و شهر سیاتل بود. کرم به طرز حیرت آوری سریع عمل کرده و تنها در عرض ۱۰ دقیقه به ۹۰ درصد از تمام سیستم های آسیب پذیر ممکن گسترش یافت (بیش از ۷۵ هزار کامپیوتر)

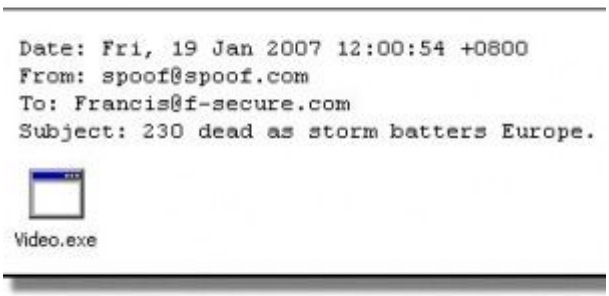
۷- Code Red
منبع احتمالی انتشار: ایالات متحده آمریکا
سال انتشار : ۲۰۰۱

این کرم که خطرناک ترین آلودگی ممکن در زمان خود محسوب می شد، با آلوده کردن رایانه های متعدد و متحد کردن آنها در حمله علیه وب سایت کاخ سفید برای خود نامی هراس انگیز دست و پا کرد. کرم نیازی به فایل اجرایی آلوده نداشت، و از طریق صدها هزار شبکه، که عمدتا متعلق به شرکت ها بود گسترش یافت.

۶- Storm

منبع احتمالی انتشار: اروپا

سال انتشار: ۲۰۰۷



کرم «طوفان» ۵۰ میلیون رایانه را آلوده کرد. این بدافزار در پیوست یک نامه الکترونیکی با عنوان "۲۳۰ کشته در جریان طوفان در اروپا " پنهان شده بود. هر چند برخی تغییرات در قالب و متن این ایمیل در رایانه

های مختلف مشاهده شده، از جمله یک مورد خبر زلزله در چین در زمان برگزاری بازی های المپیک پکن. کرم برای سوء استفاده طراحی شده و در طراحی آن از بروز رفتار غیرعادی در کامپیوتر میزبان غفلت شده بود. این کرم دکمه هایی که کاربر روی صفحه کلید را فشار می داد ثبت کرده و یک پایگاه داده بزرگ از اطلاعات محرمانه به منظور فروش اطلاعات قربانی تولید می کرد. کرم بسیار زیرک بود و بر یک کد تکیه داشت که هر ۳۰ دقیقه تغییر شکل می داد. این ویروس از این نظر که آینده بدافزار های مخرب را ترسیم می کرد و هدفش تبدیل قربانیان به خوراکی آماده برای اسپمرها (فرستندگان هرزنامه) بود، حائز اهمیت است.

۵- Mydoom

منبع احتمالی انتشار: روسیه

سال انتشار : ۲۰۰۴

Figure 1: A brief overview of WORM_MYDOOM.EA

Mydoomسریعترین کرم گسترش یافته در اینترنت بود که تا ان زمان طراحی شده بود. این کرم توسط یک فرستنده ایمیل های اسپم مأموریت یافته بود که ایمیل های ناخواسته یا اسپم حاوی پیام: "اندی ، من فقط کارم را انجام می دهم، هیچ دلبستگی شخصی در میان نیست. متأسفم!" را برای قربانیان ارسال کند .کرم اجازه کنترل از راه دور سیستم میزبان را به مهاجم می داد. برخی از گونه های حمله به وب سایت های خاصی از جمله مایکروسافت و گروه سازمان همکاری های شانگهای (SCO) انجام گرفت. برخی کارشناسان بر این باورند که کرم همچنین از طریق Kazaa خود را گسترش می دهد.

۴- Nimda

منبع احتمالی انتشار: نامعلوم

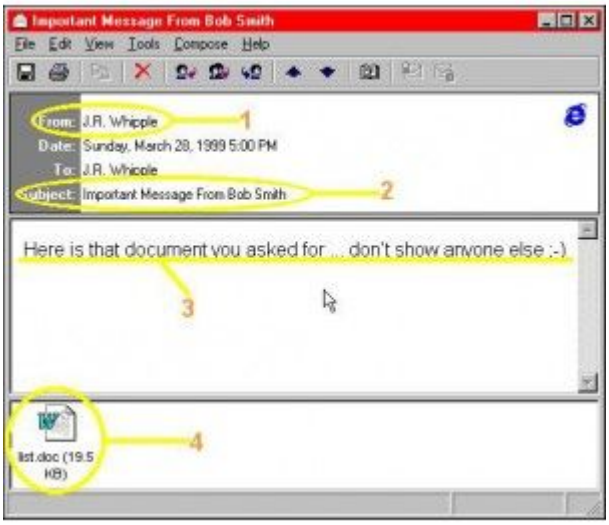
سال انتشار: ۲۰۰۱

ویروس Nimda یکی از پیچیده ترین بدافزارها در طول تاریخ است، چرا که به پنج روش مختلف خود را تکثیر می نمود. هنگامی که کامپیوتری به این ویروس آلوده می شد، ویروس یک حساب کاربری مدیریتی (Administrator Account) ایجاد کرده و اطلاعات ذخیره شده روی هارد و شبکه را با فایل های بی ارزش خود بازنویسی کرده و از بین می برد. این ویروس هر دو نوع رایانه های شخصی و سرورها را آلوده کرده و برای آلودگی نیازی به اجرای فایل برنامه توسط میزبان نداشت.

۳- Melissa

منبع احتمالی انتشار: ایالات متحده آمریکا

سال انتشار: ۱۹۹۹



این یکی در میان ماکرو ویروس ها نیرومندترین است. «ملیسا» –که نام خود را از یکی از رقاصه های عجیب و غریب از ایالت فلوریدا گرفته بود– در فایل های ایجاد شده توسط ورد، اکسل و اوت لوک نفوذ می کرد. یکی از اولین ویروس هایی بود که از طریق ایمیل گسترش می یافت و به مراتب گستردگی بیشتری نسبت به بقیه این نوع ویروس ها داشت. ملیسا بیش از یک میلیون کامپیوتر را در امریکای شمالی آلوده کرده. از جمله عوامل اصلی در هراس عمومی از فایل های ضمیمه شده در ایمیل ها همین ویروس بود. این ویروس شبکه های شرکت ها و نهادهای دولتی را آلوده کرده و دو دوره را در تاریخ بدافزارها بنیان نهاد :یکی دوره جدید ظهور ویروس ها و دیگری رویکرد جدید صنعت آنتی ویروس های مقابله کننده با بدافزارها.

I LOVE YOU –۲

منبع احتمالی انتشار: ایالات متحده آمریکا

سال : ۲۰۰۰

در آغاز دهه اول قرن بیست و یکم با تمام بدبینی های پیش زمینه کاربران، ویروس I LOVE YOU میلیون ها کامپیوتر را در یک شب آلوده کرد. این بدافزار یک اسب تروجان روی رایانه قربانی دانلود می کرد که به دنبال رمزعبور و نام های کاربری کاربر گشته، و کارهایی از قبیل بازنویسی و انتقال فایل ها را انجام می داد. ویروس توسط یک دانشجوی فیلیپینی ایجاد شده، از طریق ایمیلی با عنوان بی رحمانه " دوستت دارم" گسترش می یافت. در زمان اوج شیوع سراسری این ویروس ، تخمین زده شد ۱۰ میلیارد دلار به رایانه های خانگی و شرکت ها خسارت وارد شده است. روش های هیجان انگیز و پیچیده ویروس "دوستت دارم" موضوع ده ها پایان نامه دانشجویی و نمایشگاه امنیت رایانه ای در بسیاری از کشورهای جهان شد.

۱- Conficker
منبع احتمالی انتشار: اروپا
سال انتشار: ۲۰۰۹

کرم رایانه ای که به بیش از ۲۰۰ کشور جهان گسترش یافته و دهها میلیون رایانه و سرور را آلوده کرده و به آنها آسیب رساند، چیزی نیست جز کرم Conficker که لقب زهرآگین ترین کرم تمام دوران را از آن خود کرده است. Conficker تکنیک های مختلف نرم افزارهای مخرب را با هم ترکیب نموده و در اصل نیمه ویروس و نیمه تروجان بود.کرم تلاش می کرد تا از به روز رسانی سیستم ها جلوگیری کرده و به برنامه های ضد تروجان حمله و آنها را غیرفعال کند. Conficker به ویژه در اروپا اثرات ویرانگری از خود بر جای گذارد. از جمله خسارات قابل توجه می توان به وزارت دفاع بریتانیا، نیروی دریایی فرانسه و پلیس نروژ اشاره کرد. انتشار چندین گونه از این کرم باعث شد تا آن یک قدم جلوتر از تلاش ها برای محو آن باشد. این ویروس همچنان به عنوان بی رحم ترین برنامه مخرب موثر در دوران مدرن رایانه باقی مانده است.

تقسیم بندی ویروس های کامپیوتری بر اساس نوع آنها

به طور کلی نمی‌توان تقسیم بندی دقیقی بر روی ویروس ها ارائه داد اما می‌توان برنامه های مخرب (به طور عام ،ویروس ها) را به روش های مختلفی تقسیم بندی کرد.

تقسیم بندی برنامه های زیان آور بر اساس نوع:

۱- ویروس Virus

۲- کرم Worms

۳- تراوا Trojans

۴- در پشتی Backdoor

۵- برنامه تبلیغاتی Adware

۶- جاسوس‌افزار Spyware

۷- دانلود کننده Downloader

۸- شماره گیر Dialer

۹- برنامه خنده آور Joke

۱۰- شوخی فریبنده Hoax

۱۱- کلیک کننده Adclicker

۱۲- پسورد دزد Password-Stealer

۱۳- درآور Dropper

۱۴- تزریق‌کننده Injector

۱۵- ارسال کننده هرز نامه Spammer

۱۶- گزارش گیر صفحه کلید Keylogger

۱۷- روبات نرم افزاری Bot

۱۸- تولیدکننده‌ویروس Kits-Virus Generators

۱۹-اکسپلیوت Exploit

۲۰- روت کیت Rootkit

۱- ویروس Virus :

ویروسهای کامپیوتری برنامه‌هایی هستند که مشابه ویروس‌های بیولوژیک گسترش یافته و پس از وارد شدن به کامپیوتر اقدامات غیرمنتظره‌ای را انجام می‌دهند. با وجود اینکه همهٔ ویروس‌ها خطرناک نیستند، ولی بسیاری از آنها با هدف تخریب انواع مشخصی از فایل‌ها، برنامه‌های کاربردی و یا سیستم‌های عامل نوشته شده‌اند.

برای اینکه یک برنامه به عنوان ویروس شناخته شود فقط کافیست که آن برنامه در ساختار خود دارای یک قسمت تکثیر کننده باشد که برنامه را تکثیر کند تا بتواند سایر برنامه‌های دیگر را آلوده کند. اما در واقع ویروس‌ها در ساختار خود دارای ۴ قسمت اصلی می‌باشند:

واحد پنهان‌کننده :

یک برنامه گمراه‌کننده که باعث می‌شود ویروس بتواند خود را در کامپیوتر پنهان کند.

واحد تکثیرکننده:

یک برنامه تکثیرکننده که بوسیله آن ویروس می‌تواند خود را تکثیر کرده و برنامه‌های بیشتری را آلوده کند.

واحد فعال‌کننده:

یک کلید فعال کننده که باعث می‌شود ویروس در زمان خاصی یا بعد از انجام عمل خاصی فعال شود.

واحد اجرایی:

قسمت اجرایی ویروس که ممکن است فقط یک نمایش بدون خطر باشد و یا یک برنامه خطرناک که باعث وارد شدن صدمه به سیستم شود.

انواع ویروس

انواع ویروس‌های رایج را می‌توان به دسته‌های زیر تقسیم‌بندی نمود:

الف) ویروس‌های قطاع راه انداز

ب) ویروس‌های ماکرو

ج) ویروس‌های چندریخت

د) ویروس‌های فایل

ه)ویروس‌های مخفی

الف) ویروس‌های قطاع راه انداز :

قطاع راه‌انداز، اولین قطاع بر روی فلاپی و یا دیسک سخت کامپیوتر است. در این قطاع کدهای اجرایی ذخیره شده‌اند که فعالیت کامپیوتر با استفاده از آنها انجام می‌شود. با توجه به اینکه در هر بار بالا آمدن کامپیوتر قطاع راه‌انداز مورد ارجاع قرار می‌گیرد، و با هر بار تغییر پیکربندی کامپیوتر محتوای قطاع راه‌انداز هم مجددا نوشته می‌شود، لذا این قطاع مکانی بسیار آسیب‌پذیر در برابر حملات ویروس‌ها می‌باشد.

این نوع ویروس‌ها از طریق فلاپی‌هایی که قطاع راه‌انداز آلوده دارند انتشار می‌یابند. قطاع راه‌انداز دیسک سخت کامپیوتری که آلوده شود توسط ویروس آلوده شده و هر بار که کامپیوتر روشن می‌شود، ویروس خود را در حافظه بار کرده و منتظر فرصتی برای آلوده کردن فلاپی‌ها می‌ماند تا بتواند خود را منتشر کرده و دستگاه‌های دیگری را نیز آلوده نماید. اینگونه ویروس‌ها می‌توانند به گونه‌ای عمل کنند که تا زمانی که دستگاه آلوده‌است امکان بارگذاری کامپیوتر از روی دیسک سخت از بین برود.

این ویروس‌ها بعد از نوشتن بر روی متن اصلی بارگذاری سعی می‌کنند کد اصلی را به قطاعی دیگر بر روی دیسک منتقل کرده و آن قطاع را به عنوان یک قطاع خراب علامت‌گذاری می‌کند.

ب) ویروس‌های ماکرو :

این نوع ویروس‌ها مستقیما برنامه‌ها را آلوده نمی‌کنند. هدف این دسته از ویروس‌ها فایل‌های تولید شده توسط برنامه‌هایی است که از زبان‌های برنامه‌نویسی ماکرویی مانند مستندات اکسل یا ورد استفاده می‌کنند. ویروس‌های ماکرو از طریق دیسک‌ها، شبکه و یا فایل‌های پیوست‌شده با نامه‌های الکترونیکی قابل گسترش می‌باشد. ویروس تنها در هنگامی امکان فعال شدن را دارد که فایل آلوده

باز شود، در این صورت ویروس شروع به گسترش خود در کامپیوتر نموده و سایر فایل‌های موجود را نیز آلوده می‌نماید. انتقال این فایل‌ها به کامپیوترهای دیگر یا اشتراک فایل بین دستگاه‌های مختلف باعث گسترش آلودگی به این ویروس‌ها می‌شود.

ج) ویروس‌های چندریخت :

این ویروس‌ها 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 ویروس‌ها دشوار است.

د) ویروس‌های فایل :

تکه کدهایی هستند که خود را به فایل‌های اجرایی، فایل‌های درایور یا فایل‌های فشرده متصل می‌کنند و زمانیکه برنامه میزبان اجرامی‌گردد، فعال می‌شوند. پس از فعال شدن، ویروس با چسباندن خود به برنامه‌های موجود دیگر در سیستم گسترش می‌یابد و پخش می‌شود و همچنین کارهای بدخواهانه‌ای را انجام می‌دهد که برای آن برنامه ریزی شده‌است. اکثر ویروس‌های فایل با لود کردن خودشان در حافظه سیستم و جستجوی برنامه‌های دیگر موجود در هارد دیسک، گسترش می‌یابند. اگر برنامه‌ای را بیابند، کد برنامه را به گونه‌ای تغییر می‌دهند که در صورت اجرای مجدد آن برنامه، ویروس فعال شود. این کار بارها و بارها تکرار می‌شود تا جائیکه ویروس‌ها در سراسر سیستم و احتمالاً در سیستم‌های دیگری که در ارتباط با این برنامه آلوده هستند، منتشر شوند.

ه)ویروس‌های مخفی :

این ویروس‌ها سعی می‌کنند خود را از سیستم‌عامل و نرم‌افزارهای ضدویروس مخفی نگه دارند. برای این کار ویروس در حافظه مقیم شده و حائل دسترسی به سیستم‌عامل می‌شود. در این صورت ویروس کلیه درخواست‌هایی که نرم‌افزار ضدویروس به سیستم‌عامل می‌دهد را دریافت می‌کند. به این ترتیب نرم‌افزارهای 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 می‌دهند

۲- کرم Worms :

Worm ها نوعی ویروس هستند که اکثراً قابلیت تخریب به شکلی که فایلی را از بین ببرند ندارند . یکی از اصلی ترین ویژگیهای کرم، این است که می تواند به خودی خود تکثیر شود. اما فرآیند تکثیر در ویروسها به این صورت است که می باید فایل به جای دیگری کپی شود. در حالیکه یک کرم می تواند این کارها را به تنهایی انجام دهد.

نحوه کار Worm اغلب به این شکل است که در حافظه اصلی کامپیوتر (Ram) مستقر می شوند و شروع به تکثیر خودشان می کنند که این عمل موجب کند شدن سیستم و کم شدن تدریجی فضای Ram می گردد. کرم ها این قابلیت را نیز دارند که برای آلوده کردن کامپیوترهای دیگر از ایمیل یا برنامه های چت استفاده می کنند .

شاید بتوان گفت، اولین و مشهورترین ویروس یک Worm می باشد که به طور تصادفی در ۲ نوامبر ۱۹۸۸ وارد شبکه گردید. طبق ادعای طراح آن هدف از این کار تنها اثبات کردن ضعف سیستم امنیتی کامپیوترها بوده است. اینترنت در سال ۱۹۸۸ دوران کودکی خود را طی می کرد و تنها در اختیار محدودی از دانشگاه موسسات تحقیقاتی دولتی مانندNASA و آزمایشگاههای بین المللی مانندLos Alamos بود .با وجود اینترنت بسیار محدود آن زمان خبر از کار افتادن این مغزهای کامپیوتری درMIT وBerkeley و... تمام مردم را شوکه کرد. تنها در مدت چند ساعت بیش از ۳۰۰۰ کامپیوتر در مهمترین مراکز آمریکا از کار افتاده و خسارت وارد بر آنها در حدود ۱۰۰ میلیون دلار بر آورد گردید.

Worm ها زیر مجموعه ای از ویروسهای کامپیوتری می باشند که بر خلاف دیگر ویروسها از جملهMelissa که خود را به صورتE-Mail برای کاربران اینترنتی می فرستد سیستم کامپیوتر را سوراخ کرده و به طرف مغز کامپیوتر پیش می روند یکی از خصوصیات بارزWormها توانایی پنهان شدن درون سیستم بوده بطوریکه قابل ردگیری نمی باشند این Worm ها مانند ویروسهایی می باشند که خود را در اعصاب ستون فقرات پنهان کردن و گاه و بی گاه دردهای شدیدی را تولید

می کنند. و اماWorm های مفید : در میان انـواعWorm هـا کرمهـای مفیـدی نیـز طـی سـالیان متمادی به منظور چک کردن کارایی سیستم و ... مورد استفاده قرار گرفته اند.

اینWorm ها Agent نامیده شده و درون شبکه حرکت کرده اطلاعات منابع مورد اسـتفاده و ... را چک و اطلاعاتی در مورد کارکرد شبکه یا حتی محلی را که می توان ارزانتـرین DVD را خریـداری نمود به کاربر اعلام می دارند از تفاوتهای بارز میانAgent و Worm می توان به این مـورد اشـاره کرد که Agent بر خلاف Worm خود را تکثیر نکرده و درون سیستمهای کاربران نفوذ نمی کند.

تاریخچه اولین کرم رایانه ای Worm

این Worm که توسـط Robert Tappan Morris طراحـی شـد بـه RTM مـشهور گردید . Morris بعد از اتمام دوره لیسانس خود در پاییز سال ۱۹۸۸ از دانشگاه خارج و بـه برنامه نویسی کامپیوتر روی آورد بعد از آن در مقطع Ph.D دانشگاه MIT در رشته مـورد علاقه خود مشغول به تحصیل گردیـد و بـدین ترتیـب از امکانـات کـامپیوتری و اینترنتـی دانشگاه بهره مند شد . وی در اکتبر سال ۱۹۸۸ برنامه ای را به منظور پی بـردن بـه نقـاط ضعف سیستمهای اینترنتی و امنیتی کامپیوتر طراحی کـرد . نحـوه کـار ایـن برنامـه بـدین ترتیب بود که پس از رها شدن آن در اینترنت سریعاً و بدون جلب هیچ گونه توجهی پخش می گشت (طبق اظهارات وکیل مدافع موریس)

موریس به منظور جلوگیری از مشخص شـدن هویـت خـود پـس از اتمـام برنامـه آن را از طریق کامپیوترهای دانشگاه MIT وارد شبکه کرد. یکی از خصوصیات این ویروس اضـافه کردن یک شمارنده به برنامه بود. بدین ترتیب در صورتیکه این برنامه حداکثر تا ۶ بار یـک کپی از خود را در کامپیوتر پیدا می کرد تکثیر نشده و در هفتمـین بـار ایـن برنامـه پـس از تکثیر و نفوذ به کامپیوتر آن را مورد هجوم قرار می داد. ایـن برنامـه ضـمیمه یـک اشـتباه بسیار مهلک بود!! کامپیوترهایی که در سال ۱۹۸۸ به اینترنت متـصل مـی شـدند بـه طـور میانگین هر ۱۰ روز یکبار خاموش شده و دوباره راه اندازی می گـشتند از آنجـا کـه برنامـه موریس در کامپیوتر ذخیره نمی شد این خصوصیت سوپاپ اطمینانی گشت تـا بـه هـر بـار

خاموش شدن کامپیوتر برنامه به طور خودکار از میان برود. با این حال از آنجایی کـه تمـام کامپیوترهای متصل به اینترنت به طور همزمـان خـاموش نمـی شـدند ایـن Worm مـی توانست دوباره برگشته و در آنجا مقیم گردد. طبق این نظریه مـوریس، تعـداد Worm هـا همواره دارای یک تعادل بوده و مشکل خاصی را در کامپیوتر سبب نمی شـدند. و امـا ایـراد برنامه موریس در این بود که این Worm بسیار سریعتر از انتظار موریس تکثیر مـی یافـت در کمتر از چند ساعت بعد از آزاد سازی آن هزاران کامپیوتر در مراکز حساس از کـار افتـاده و دچار سکته شدند. پنج روز بعد از آزاد سازی worm در ۶ام نـوامبر همـه چیـز بـه حالـت عادی خود برگشت در روز ۱۲ توامبر سرانجامE-Mail هـایی کـه مـوریس در آنهـا طـرز خنثی کردن Wrom را توضیح داده بود به مقاصـد خـود رسـیده و مـردم از نحـوه خنثـی سازیWorm آگاهی یافتند.

کرم ها از کجا می آیند؟

اکثر این کرم ها از ضمیمه های ایمیل ها می آیند. احتمالاً این مطلب را هم قبلاً شنیده اید، اما باز کردن ضمیمه ی ایمیل ها از آدرس های ناشناس، اصلاً ایده ی خوبی نیست. برخی ازکرم ها ممکن است حتی از آدرس های کامپیوترهای آلوده (مثلاً کامپیوتر دوستتان) برای نفوذ استفاده کنند. این نوع کرم ها از تمام اتصالات کامپیوتر آلوده استفاده میکنند. این بدان معناست که ممکن است شما یک ایمیل خطرناک از کسی که فکر می کنید قابل اعتماد است، دریافت کنید. حتی فایلهای wordو یا excel هم می توانند در قالب ماکروها حاوی کرم باشند.

کرم هایی که خطرناک نیستند

از زمانیکه که کرم ها اختراع شدند، برخی از آنها واقعاً با هدف آسیب نرساندن به سیستم، ساخته شدند. تعداد اندکی از آنها، مانند کرم های خانواده ی ناچی (Nachi Family) ، در حقیقت سعی می کنند یک نرم افزار امنیتی را دانلود و نصب کند تا منفذی را که از آن وارد شده اند ، ترمیم کنند. کرم ها معمولاً بخشهای خطرناکی از ویروسها (malware)

هستند و می توانند به اندازه ی ویروسهای قدیمی مضر باشند. پس باید در مقابل آنها مراقب بود.

۳- تروا (تروجان) Trojans :

اسب‌های تروآ خود را به شکل نرم‌افزارهای سودمندی در می‌آورند که برای دانلود کردن در اینترنت لازم‌اند، و کاربران ساده و بی خبر آنها را دانلود کرده و به اجرا در می‌آورند و بعداً متوجه اشتباه خود می‌شوند. بزرگ‌ترین تفاوت بین اسب تروآ و یک ویروس این است که تروآها خودشان منتشر نمی‌شوند.

اسب تروآ معمولاً به دو بخش سرویس دهنده و سرویس گیرنده تقسیم می‌شود و خود را به شکل یک نرم‌افزار مهم در می‌آورد و در شبکه‌های به اشتراک گذاری فایل نظیر به نظیر یا سایت‌های غیررسمی دانلود ، قرار می‌گیرد. زمانی‌که سرویس گیرنده در سیستم شما اجرا می‌شود. حمله کننده (شخصی که سرویس دهنده را اجرا می‌کنند) دسترسی بالایی بر روی سیستم شما دارد، و می‌تواند بسته به نیت و هدف حمله کننده تأثیرات تخریبی داشته باشد. اسب‌های تروآ به یک تراز بسیار پیچیده رسیده‌اند که موجب شده هر کدام بطور قابل ملاحظه‌ای متفاوت از دیگری باشد.

انواع تروجان

اسب‌های تروآ معمولاً به این صورت طبقه بندی می‌شود:

الف) تروآهای دسترسی از راه دور

ب) تروآهای ارسال کننده رمز عبور

ج) ترآواهای ثبت کننده کلید

د) تروآهای حملهٔ سرکاری

ه)تروآهای پروکسی

و) تروآهای اف تی پی

الف) تروآهای دسترسی از راه دور

این تروآها از نوع بسیار متداول هستند. حمله کننده بااستفاده از آنها می‌توانند کنترل کاملی بر روی کامپیوترهای قربانی داشته باشد. حمله کننده می‌توانند به داخل فایل‌ها برود و به هر گونه اطلاعات شخصی کاربر همچون اسناد مالی مهم، رمزهای عبور، شماره کارت اعتباری و از این قبیل که ممکن است در فایل‌های ذخیره شده باشند، دسترسی یابد.

ب) تروآهای ارسال کننده رمز عبور

هدف این تروآها کپی کردن تمام رمزهای عبور کش شده و جستجوی رمزهای عبور دیگری که وارد می‌کنید و ارسال آنها به آدرس ایمیل خاص است، بدون آنکه کاربر متوجه شود. رمز عبور وب سایت‌های محدود شده، سرویس‌های پیغام رسانی، و سرویس‌های ایمیل در معرض تهدید این نوع تروآها هستند.

ج) ترآواهای ثبت کننده کلید

این نوع تروجان، کلیدهایی که توسط قربانی فشرده می‌شوند را ثبت می‌کنند و سپس اطلاعات ثبت شده را به حمله کننده ارسال می‌دارند. حمله کننده، به جستجوی رمزهای عبور یا اطلاعات حساس دیگر در فایل‌های ثبت وقایع می‌پردازد. این نوع تراوآ اکثرا دو ویژگی دارند: ثبت آنلاین و آفلاین. البته آنها می‌توانند طوری تنظیم شوند که فایل ثبت وقایع را به یک آدرس ایمیل خاص به صورت روزانه ارسال کنند.

د) تروآهای حملهٔ سرکاری

ایدهٔ اصلی این نوع تروآها ایجاد ترافیک شبکه در دستگاه قربانی است، تا جائیکه ارتباط اینترنتی بسیار سنگین شده و مانع از آن می‌شود که کاربر یک وب سایت را ببیند. یا چیزی را دانلود کند. نوع دیگر از این تراوآ، تروآی بمب پستی است، که هدف اصلی آن آلوده کردن ماشین‌ها تا حد امکان و همزمان حمله به آدرس‌های ایمیل خاص با موضوعات و محتویات اتفاقی است که قابل فیلتر شدن نیستند.

ه)تروآهای پروکسی

این نوع تروآ کامپیوتر قربانی را به یک سرویس دهنده پروکسی تبدیل می‌کند. به این ترتیب کامپیوتر آلوده در دسترس اشخاص ناشناس در سراسر جهان قرار می‌گیرد. حمله کننده می‌تواند حوزه‌ها را ثبت کند یا با کارت‌های اعتباری به سرقت رفته شده به وب سایت‌ها دسترسی یابد یا اینکه کارهای غیرقانونی دیگری را انجام دهد بدون آنکه ردیابی شود.

و) تروآهای اف تی پی

این تروآها بسیار ساده و منسوخ شده‌اند. تنها کاری که انجام می‌دهند باز کردن پورت ۲۱ است. (این پورت مربوط به انتقالات اف تی پی است) و موجب می‌شود تا هر کسی به دستگاه شما وصل شود. در نسخه‌های جدیدتر این پورت با رمز عبور محافظت می‌شود، بنابراین تنها حمله کننده می‌تواند به کامپیوتر شما وصل شود.

یک تروآ می‌تواند شامل یک یا ترکیبی از عملکردهای فوق‌الذکر باشد .

۴- در پشتی Backdoor :

برنامه ای است که به یک نفوذ گر این امکان را می دهد تا پروسه امنیتی یک سیستم را دور زده و منابع مختلفی از آن سیستم را از راه مربوطه در اختیار نفوذ گر قرار دهد.

تعداد بسیار زیادی از انواع در های پشتی قابل ذکر می باشد همانطور که طبق تعریف بالا مشاهده می کنید مبنای اصلی که به یک در پشتی مربوط می شود به دستیابی یک نفوذ گر به منابع سیستمی از طریق در پشتی تعریف می شود.این دسترسی می تواند به شکل های گوناگونی صورت گیرد که این موضوع بستگی به هدفی دارد که هکر از به کار گیری درهای پشتی دنبال می کند به طور مثال :

تغییر در سطح دسترسی محلی :

این نوع درپشتی به نفوذ گر این امکان را می دهد که ناگهان یک حساب کاربری معمولی به حساب کاربری با دسترسی به Administratorیا Root تبدیل شده و ارتقاء یابد بـا

این دسترسی نامحدود نفوذ گر می تواند دوباره فایل های ذخیره شده بر سیستم را به روش خود پیکر بندی نماید.

اجرای فرمانهای منفرد از راه دور:

در این نوع ار درهای پشتی هکر می تواند با ارسال پیغام به سیستم هدف در همان لحظه یک تک فرمان را بروی ماشین مورد نظر اجرا کند در پشتی فرمان تکی هکر را اجرا کرده و نتیجه را به هکر باز می گرداند.

دسترسی به یک سطر فرمان از سیستم هدف از راه دور :

این یکی از شناخته شده ترین در های پشتی برای هکر ها می باشد نام معروف این نوع Remote Shell است. در این نوع در پشتی به هکر این امکان را می دهد در سطر فرمان سیستم قربانی و از طریق شبکه فرمانهایی را به طور مستقیم اجرا نماید در این نوع نفوذگر می تواند سطر فرمان را به یک ابزار کاربردی تبدیل نماید. از جمله، توانایی انجام یک سری فرمان ها به طور موازی و یا نوشتن Script های خطرناک و یا انتخاب دسته ای از فایل ها برای جمع‌آوری آن فایلها.با بررسی بیشتر می‌توان گفت Remote Shellها بسیار پر توان تر و پر کاربرد تر از اجرای فرمان های تکی بر روی که سیستم هدف می‌باشند به تشابهی، این نوع در پشتی یک دسترسی مستقیم به کی‌بورد سیستم هدف برای نفوذگر تهیه می نماید.

دسترسی از راه دور به ماشین هدف از طریق برنامه های GUI:

بعد از گذراندن مراحل دسترسی های سطر فرمان به ماشین هدف به در های پشتی می رسیم که یک دسترسی به GUI از سیستم هدف را برای ما تهیه می‌نمایند. به طور مثال باز و بسته شدن پنجره ها یا حرکت ماوس و ... در این نوع شما می توانید نظاره گر فعالیتهای قربانی بر روی سیستم اش باشید یا خود می توانید کنترل GUI سیستم مورد نظر را در دست بگیرید.

۵- برنامه تبلیغاتی Adware :

Adware ها ، برنامه های مخربی هستند که تبلیغات ناخواسته برای کاربران می فرستند و نسبت به سایر بدافزارهای اینترنتی شیوع بیشتری یافته اند. به واقع نمی توان هیچ کاربر اینترنتی را پیدا کرد که حداقل با یک نوع Adware برخورد نکرده باشد.

گونه های مختلف adware به نحوی به سیستم کاربر نفوذ می یابند که کاربر متوجه آنها نشود البته ورودشان به یک سیستم کاملا با اجازه کاربر صورت می گیرد، به نحوی که درخواست آنها برای نصب ، در غالب یک برنامه کاملا بی خطر انجام می گیرد و کاربر بدون توجه به غیر واقعی بودن آن برنامه ، درخواست مذکور را قبول می کند.

Adware ها پس از ورود، به یک سرور خارجی متصل می شوند که به وسیله آن تبلیغات مشخصی به سیستم آلوده ارسال می کنند. نحوه عملکردشان به گونه ای است که زمانی که کاربر به اینترنت وصل می‌شود، Adware مذکور به یک کامپیوتر دیگر متصل می شود و تبلیغاتی را به صورت pop-up بر روی صفحه نمایش، اجرا می کند. اغلب کاربران متوجه نمی شوند که این pop-up ها مربوط به وب سایتی است که مشاهده می کنند یا از طریق یک adware که کامپیوترشان را آلوده کرده، برایشان ارسال شده. این عملکرد به خودی خود برای کاربران مضر است به این دلیل که ارتباط کاربر را با اینترنت بسیار کند می کند. ضمنا از آنجا که adware ها اغلب spyware ها یی را که علاقمندیهای کاربر را جمع آوری می کنند همراه خود دارند می توانند اطلاعات سیستم آلوده شده را روی سرورهای خود بفرستند. برای مثال اگر شما در اینترنت مرتبا به دنبال سایت های باغبانی بگردید، adware نصب شده روی سیستمتان دائما برای شما تبلیغاتی که مربوط به گل و گیاه است می فرستد.

یک مثال خوب برای نشان دادن نحوه عملکرد adware ها بررسی Twain-Tech است. این adware به شکل " پرداخت " برای یک برنامه کاربردی به سیستم کاربر نفوذ می کند و پس از نصب دائما pop-up های تبلیغاتی روی صفحه، نمایش می دهد. محتوای این تبلیغات بستگی به

وب پیج هایی دارد که کاربر غالبا مشاهده یا جستجو می کند. کار دیگری که این برنامه مخرب انجام می دهد دانلود کردن spyware ها و انواع دیگری از adware ها مانند Alchemy, Xplugin, و BetterInet است.

مبارزه با Adware ها

به دلیل شیوع گسترده این بدافزارها در اینترنت، رهائی از دست آنها کاری مشکل است. مخصوصا برای سیستم هایی که آنتی ویروس مناسبی ندارند. هم چنین از آنجا که نویسندگان این کدهای مخرب با دستیابی به اهداف مالی، آنها را منتشر می کنند، دائما سعی می کنند نمونه های پیچیده تر و جدیتر از مدلی های قبلی را منتشر کنند.

در نتیجه بهترین راه حل نصب یک آنتی malware همراه یک فایروال است که دائما به روز شود. این کار باعث می شود نه تنها از ورود adware ها به سیستم جلوگیری شود بلکه راه ورود و خروج اطلاعات از پورت های محافظت نشده نیز بسته می شود.

۶- جاسوس افزار Spyware :

جاسوس افزار، واژه جدیدی برای نرم‌افزارهای تبلیغاتی است. تبلیغ محصولات اشتراک افزار روشی برای مولفین اشتراک افزار است تا به نوعی پول سازی کنند. شرکت‌های رسانه‌ای بزرگی وجود دارند که پیشنهاد می‌کنند در ازای بخشی از منافع حاصله از فروش بنر ، تبلیغات بنر را در محصولات خود قرار دهند. در صورتیکه کاربر احساس کند که این بنرها مزاحمند، این امکان برای آنها وجود دارد که در ازای پرداخت مخارج پروانه، از شر آن خلاص شوند.

متاسفانه، شرکت‌های تبلیغ کننده اغلب نرم‌افزار ردیابی کننده در سیستم شما نصب می‌کنند، و این نرم‌افزار دائماً از ارتباط اینترنتی شما استفاده می‌کند تا داده‌های آماری را به تبلیغ کننده ارسال دارد. گرچه این شرکت‌ها در سیاست‌های خصوصی خود مدعی هستند که هیچگونه اطلاعات مهم یا توصیف کننده‌ای از جانب سیستم شما گردآوری نخواهد شد و هویت شما همچنان ناشناس باقی می‌ماند، اما حقیقت این است که شما سرویس دهنده‌ای دارید که در کامپیوتر شما قرار دارد و اطلاعات مربوط به شما و عادات جستجوی شما را از طریق باند پهن به یک محل دور ارسال

می‌دارد. جاسوس افزار به دلیل استفاده تقریباً زیاد از قدرت پردازشی ، کامپیوترها را کند می‌کند، پنجره‌های آزار دهنده را در زمان‌های نامناسب ظاهر می‌نماید و تنظیمات مرور کردن اینترنتی شما را تغییر می‌دهد. مثلاً، صفحه شروع یا موتور جستجوی شما را به سرویس‌های متعلق به خودش مبدل می‌کند. حتی اگر برخی‌ها چنین چیزی را غیر قانونی ندانند، اما جاسوس افزارها همچنان یک تهدید امنیتی محسوب می‌شوند و این حقیقت که هیچ راهی برای خلاصی از آنها وجود ندارد، آنها را به اندازه ویروس‌ها آزار دهنده ساخته‌است.

۷- دانلود کننده Downloader :

این برنامه برعکس برنامه های جاسوسی کارشان دانلود برنامه های زیان آور بر روی سیستم و اجرای آنها است .

۸- شماره گیرDialer :

اینگونه برنامه‌ها وظیفه‌شان ارتباط دادن کاربر از طریق خط تلفن به سرورهایی در دیگر کشورها برای دسترسی مستقیم به اطلاعات آنها می‌باشد.

این سرورها معمولا مربوط به سایت‌های غیراخلاقی بوده و برقراری ارتباط با آنها از طریق خط تلفن باعث هزینه بسیار زیاد مالی می‌گردد.

۹- برنامه خنده آورJoke :

این برنامه نه کار تخریبی می کند و نه جاسوسی بلکه برنامه های است که باعث آزار کاربر شده و در بعضی مواقع خنده آور است . جک‌ها برنامه‌هایی هستند که ادعا می‌کنند در حال انجام عملیاتی تخریبی بر روی سیستم شما می‌باشند ولی در واقع اینگونه نبوده و کار آنها چیزی جز یک شوخی ساده نمی‌باشد.

این برنامه‌ها با سوء استفاده از کم بودن اطلاعات تخصصی کاربران، آنها را فریب داده و با دستورات و توصیه‌های اشتباه باعث می‌شوند که کاربر شخصاً کاری تخریبی بر روی سیستم خود انجام دهد. به عنوان مثال وانمود می‌کنند که فایلی خاص در مسیر سیستم عامل یک برنامه خطرناک است و

باید توسط کاربر حذف شود. غافل از اینکه این فایل سیستمی بوده و برای عملکـرد درسـت سیـستم عامل، وجود آن لازم است.

۱۰- شوخی فریبنده Hoax :

این نوع ویروسها در قالب پیغامهای فریب آمیزی ، کاربران اینترنت را گول زده و به کام خود می‌کشد. این نوع ویروسها معمولاً به همراه یک نامه ضمیمه شده از طریق پست الکترونیک وارد سیستم می‌شوند. متن نامه مسلماً متن مشخصی نیست و تا حدودی به روحیات شخصی نویسنده ویروس بستگی دارد، پیغامها می توانند مضمونی تهدید آمیز یا محبت آمیز داشته باشند و یا در قالب هشداری ، مبنی بر شیوع یک ویروس جدید در اینترنت ، یا درخواستی در قبال یک مبلغ قابل توجه و یا هر موضوع وسوسه انگیز دیگر باشد . لازم به ذکر است که همه این نامه‌ها اصل نمی‌باشند یعنی ممکن است بسیاری از آنها پیغام شخص سازنده ویروس نباشند بلکه شاید پیغام ویرایش شده یا تغییر یافته از یک کاربر معمولی و یا شخص دیگری باشد که قبلا این نامه‌ها را دریافت کرده و بدینوسیله ویروس را با پیغامی کاملاً جدید مجدداً ارسال می‌کند.نحوه تغییر پیغام و ارسال مجدد آن بسیار ساده بوده ، همین امر باعث گسترش سریع Hoaxها شده، با یک دستور Forward می‌توان ویروس و متن تغییر داده شده را برای شخص دیگری ارسال کرد.

۱۱- کلیک کننده Adclicker

اینگونه برنامه‌ها لینک صفحات تبلیغاتی را دنبال نموده و به این طریق حالت کلیـک شـدن بـر روی آن صفحه تبلیغاتی خاص را شبیه سازی می کنند و باعث بالا رفتن hit آن می شوند.

۱۲- پسورد دزد Password-Stealer

نوعی ترویا هستند کارشان دزدی پسورد از روی سیستم ها و ارسال آنها برای نفوذگرها است.

۱۳- درآور Dropper

هر نوع برنامه بد افزار دیگر را از دل خود بیاورند بیرون می آورند و به خودی خود اثرات تخریبی ندارند.

۱۴- تزریق‌کننده Injector

به برنامه های موجود در حافظه تزریق می شوند و از طریق آنها منتشر می شوند و به تنهایی قدرت انتشار ندارند.

۱۵- ارسال کننده هرز نامه Spammer

این نوع برنامه ها باعث ارسال ایمیل های نا مربوط (Spam) برای کاربران اینترنتی.

۱۶- گزارش گیر صفحه کلید Keylogger

اینگونه برنامه ها با قرار گرفتن در حافظه از کلید های زده شده توسط کاربر گزارش گرفته و در قالب یک فایل برای نفوذگر می فرستند.

۱۷- روبات نرم افزاری Bot

نوعی روبات های نرم افزاری هستند که با استفاده از نرم افزار های چت با کاربران اینترنتی چت می‌کنند . البته شاید بتوان این نوع برنامه ها را از این لحاظ جزء بد افزار ها دسته بندی کرد که باعث اتلاف وقت کاربران می‌شوند.

البته نوع دیگری هم از این نوع وجود دارند که یک روبات نرم افزاری هوشمند است که به طور مستمر در حال پیمایش اینترنت و جمع آوری اطلاعات منتشر شده در این شبکه جهانی است. این اطلاعات را پیگیری و سپس تجزیه و تحلیل می کند و نتیجه هایی را که پیش گویی کرده ارائه می‌دهد. تولد وب بات به سال ۱۹۹۷ بر می گردد؛ در این سال یک برنامه نویس نابغه با نام کلیف های (Clif High) و شریک او جورج یور (George Ure) این نرم افزار را پدید آوردند. هدف اصلی آنها تجزیه و تحلیل بازار بورس بود تا بتوانند نوسان های آینده را پیش گویی کنند.

۱۸- تولیدکننده‌ویروس Kits-Virus Generators

با استفاده از این نرم افزار ها می توان ویروس تولید کرد.

۱۹-اکسپلیوت Exploit

کدهای مخربی هستند که با استفاده از آسیب پذیری های یک سیستم امکان دسترسی از راه دور به آن سیستم را فراهم می کنند.

۲۰- روت کیت Rootkit

به خودی خود نمی توان مخرب یا خطرناک باشند، بلکه قرار گرفتن آنها در کنار ویروس ها یا کرمهای اینترنتی که به آنان ماهیتی خطرناک می بخشد.

Rootkit ها ابزاری نرم افزاری است که بوسیله آن این امکان وجود دارد تا فایل، پروسه یا کلیدی خاص در رجیستری را پنهان نمود.

Rootkit ها اغلب در سطح سیستم عامل فعالیت کرده و با تغییراتی که در سیستم عامل یا منابع آن انجام می دهند، به مقاصد خود دست پیدا می کنند.

آنتی ویروس

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

نرم‌افزارهای آنتی ویروس عموما از دو تکنیک برای تشخیص ویروسها استفاده می‌کنند:

۱. استفاده از فایل امضای ویروس

۲. تحلیل آماری

استفاده از فایل امضای ویروس

این تکنیک توانایی شناسایی ویروسهایی را دارد که شرکتهای آنتی ویروس تا کنون برای آنها امضا تولید کرده‌اند. در این روش ضد ویروس متن فایلهای موجود دررایانه را هنگامی که سامانه عامل آنها را بازمی کندیامی بندد یا ارسال می‌کند امتحان می‌کند و آن را به فایل امضای ویروس که نویسندگان آنتی ویروس تشخیص داده اندارجاع می‌دهد.

فایل امضای ویروس یک رشته بایت است که با استفاده از آن می‌توان ویروس را به صورت یکتا مورد شناسایی قرار داد و از این جهت مشابه اثر انگشت انسانها می‌باشد.

اگر یک تکه کد در فایلی با ویروس موجود در فایل امضای ویروس مطابقت داشت نرم‌افزار ضد ویروس یکی از کارهای زیر را انجام می‌دهد:

الف) سعی می‌کند تا فایل را توسط از بین بردن ویروس به تنهایی تعمیر کند. ب) قرنطینه کردن فایل(فایل قابل دسترسی توسط برنامه‌های دیگر نباشدو ویروس آن نمی‌تواند گسترش یابد.)

ب) فایل ویروسی و آلوده را پاک کند.

دراین تکنیک ، فایل امضای ویروس یا همان پایگاه داده ویروسهای شناخته شده ، باید به طور متناوب بهنگام شودتا آخرین اطلاعات را راجع به آخرین ویروسها به دست آورد.

کاربران وقتی ویروسهای جدید (ناشناخته) راتشخیص دادند، می‌توانند فایل‌های آلوده را به نویسندگان یا شرکتهای آنتی ویروس ارسال کنند.

تحلیل آماری

فایل در این روش در یک محیط محافظت شده در داخل ماشین مجازی شروع به اجرا می‌کند سپس به برنامه آنتی ویروس اجازه می‌دهد تا رفتار یک فایل مشکوک را به هنگام اجرا شبیه سازی کند در حالی که کد مشکوک اصلی ازماشین واقعی کاملامجزا شده‌است. و بعد برفعالیتهای ویروسی مثل تکرار کد ، دوباره نویسی فایل ، و تلاش برای پنهان سازی فایلهای مشکوک نظارت می‌کند. هرگاه یک یابیشتر از آن فعالیتهای شبه ویروس را پیدا کرد، فایل مشکوک علامت گذاریمی شود و به کاربر اطلاع داده می‌شود. مثلا اگر برنامه‌ای از رمزخود تصحیح کننده استفاده کرده ویروس به شمار می‌آید. این تکنیک حفاظت بیشتری را در مقابل ویروسهای جدید تجاری که هنوز وارد پایگاه داده نشانه‌های ویروسی نشدند، به‌وجود می‌آورد .[۲]

فایروال چیست ؟

فایروال یک برنامه و یا دستگاه سخت‌افزاری است که با تمرکز بر روی شبکه و اتصال اینترنت ، تسهیلات لازم در جهت عدم دستیابی کاربران غیرمجاز به شبکه و یا کامپیوتر شما را ارائه می‌نماید. فایروال‌ها این اطمینان را ایجاد می‌نمایند که صرفا" پورت‌های ضروری برای کاربران و یا سایر برنامه‌های موجود در خارج از شبکه در دسترس و قابل استفاده می‌باشد. به منظور افزایش ایمنی ، سایر پورت‌ها غیرفعال می‌گردد تا امکان سوء استفاده از آنان توسط مهاجمان وجود نداشته باشد . در برخی موارد و با توجه به نیاز یک برنامه می‌توان موقتا" تعدادی از پورت‌ها را فعال و پس از اتمام کار مجددا" آنان را غیرفعال نمود . بخاطر داشته باشید که به موازات افزایش تعداد پورت‌های فعال ، امنیت کاهش پیدا می‌نماید .

فایروال‌های نرم‌افزاری ، برنامه هائی هستند که پس از اجراء ، تمامی ترافیک به درون کامپیوتر را کنترل می‌نمایند(برخی از فایروال‌ها علاوه بر کنترل ترافیک ورودی ، ترافیک خروجی را نیز کنترل می‌نمایند) . فایروال ارائه شده به همراه ویندوز اکس پی ، نمونه‌ای در این زمینه‌است . فایروال‌های نرم‌افزاری توسط شرکت‌های متعددی تاکنون طراحی و پیاده سازی شده‌است . تعداد زیادی از اینگونه فایروال‌ها، صرفا" نظاره گر ترافیک بین شبکه داخلی و اینترنت بوده و ترافیک بین کامپیوترهای موجود در یک شبکه داخلی را کنترل نمی‌نمایند.

فایروالها به دو دستهٔ فایروالهای شخصی و فایروالهای و فایروالهای شبکه تقسیم می‌شوند. کار فایروالهای شخصی محافظت از یک شبکه در مقابل شبکه دیگر است ولی فایروالهای شخصی تنها از یک کامپیوتر در مقابل یک شبکه محافظت می‌کند. شکل ۲ و شکل ۳ به ترتیب این مفاهیم را در مورد فایروالهای شخصی و فایروالهای شبکه نشان می‌دهند

انواع فایروال

فایروال‌ها به دو شکل سخت‌افزاری (خارجی) و نرم‌افزاری (داخلی) ، ارائه می‌شوند . با اینکه هر یک از مدل‌های فوق دارای مزایا و معایب خاص خود می‌باشند ، تصمیم در خصوص استفاده از یک فایروال بمراتب مهمتر از تصمیم در خصوص نوع فایروال است.

فایروال‌های سخت‌افزاری

این نوع از فایروال‌ها که به آنان فایروال‌های شبکه نیز گفته می‌شود ، بین کامپیوتر شما (و یا شبکه) و کابل و یا خط دی اس ال قرار خواهند گرفت . تعداد زیادی از تولید کنندگان و برخی از مراکز آی اس پی دستگاههائی با نام روتر را ارائه می‌دهند که دارای یک فایروال نیز می‌باشند . فایروال‌های سخت‌افزاری در مواردی نظیر حفاظت چندین کامپیوتر مفید بوده و یک سطح مناسب حفاظتی را ارائه می‌نمایند(امکان استفاده از آنان به منظور حفاظت یک دستگاه کامپیوتر نیز وجود خواهد داشت) . در صورتی که شما صرفا" دارای یک کامپیوتر پشت فایروال می‌باشید و یا این اطمینان را دارید که سایر کامپیوترهای موجود بر روی شبکه نسبت به نصب تمامی مسیرها ، بهنگام بوده و عاری از ویروس‌ها و یا کرم‌ها می‌باشند ، ضرورتی به استفاده از یک سطح اضافه حفاظتی (یک نرم‌افزار فایروال) نخواهید داشت . فایروال‌های سخت‌افزاری ، دستگاههای سخت‌افزاری مجزائی می‌باشند که دارای سیستم‌عامل اختصاصی خود می‌باشد . بنابراین بکارگیری آنان باعث ایجاد یک لایه دفاعی اضافه در مقابل تهاجمات می‌گردد.

فایروال‌های نرم‌افزاری

برخی از سیستم‌های عامل دارای یک فایروال تعبیه شده درون خود می‌باشند . در صورتی که سیستم‌عامل نصب شده بر روی کامپیوتر شما دارای ویژگی فوق می‌باشد ، پیشنهاد می‌گردد که آن را فعال نموده تا یک سطح حفاظتی اضافی در خصوص ایمن سازی کامپیوتر و اطلاعات ، ایجاد گردد .(حتی اگر از یک فایروال خارجی یا سخت‌افزاری استفاده می‌نمائید). در صورتی که سیستم‌عامل نصب شده بر روی کامپیوتر شما دارای یک فایروال تعبیه شده نمی‌باشد ، می‌توان اقدام به تهیه یک فایروال نرم‌افزاری کرد . با توجه به عدم اطمینان لازم در خصوص دریافت نرم‌افزار از اینترنت با استفاده از یک کامپیوتر محافظت نشده، پیشنهاد می‌گردد برای نصب فایروال از سی دی مربوطه استفاده گردد . شکل ۴ نحوه کار فایروالهای سخت‌افزاری و شکل ۵ نحوه کار فایروالهای نرم‌افزاری را نشان می‌دهد.

نتیجه‌گیری و جمع‌بندی

برنامه های مخرب در سه دسته عمده ویروس،کرم و تروجان قرار می‌گیرند. شمار این نرم‌افزارها بسیار زیاد و روبه افزایش است. همچنین بمب‌های منطقی، جاسوس‌افزارها، اسپم‌ها وگول‌زنک‌ها از دیگر انواع برنامه‌های

مخرب به‌شمار می‌روند. آنتی‌ویروس‌ها از دو روش کلی به منظور محافظت از کامپیوترها بهره می‌گیرند. فایروالها گونه‌ای دیگر از نرم‌افزارهایی هستند که در کامپیوترهای شخصی محافظت‌هایی را در مقابل برنامه‌های مخرب فراهم می‌آورند. فایروالها به دو دسته فایروالهای شخصی و فایروالهای شبکه تقسیم می‌شوند. برنامه‌های مخرب بسیار زیاد می‌باشند و هر روز نیز به تعداد و انواع آنان افزوده می‌شوند. برای مقابله با این برنامه‌ها وجود برنامه‌هایی نظیر آنتی‌ویروسها و فایروالها وهمچنین به‌هنگام‌سازی آنها امری ضروری است.