همه چیز درباره ویروس‌ها، کرم‌ها، اسب‌های تروا و فراتر از آن

« بخش دوم »

کلیه حقوق این مقاله متعلق به سایت امنیت وب و مترجم آن می باشد و هر گونه برداشت از آن فقط با ذکر نام سایت و نام نویسنده مجاز می باشد.

مترجم : رضا مددی / rzmadadi@yahoo.com

منبع : www.Sophos.com

تاریخ : ۱۷ اردیبهشت ۱۳۸۳

در صورتی که شما :

- **یک مدیر شبکه هستید،**
- **فردی هستید که با دوستان خود دیسک مبادله می‌کند،**
- **از شبکه‌های محل کار خود استفاده می‌کنید،**
- **و یا فقط خواننده نامه‌های الکترونیکی هستید،**

بدانید که این مطلب برای شماست!

ما حقایق را در باره ویروس‌های کامپیوتری بطور ساده و با زبانی قابل فهم برای شما بیان می‌کنیم.

فهرست مطالب

بخش اول

- چرا ویروس‌ها مهم هستند؟
- ویروس ها، اسب‌های تروا و کرم‌ها
- تعریفی ساده از ویروس، اسب تروا، کرم
- ویروس چیست؟
- ویروس چگونه بر روی کامپیوتر تاثیر می‌گذارد؟
- اسب‌های تروا
- کرم‌ها
- ویروس‌ها چه کارهایی می‌توانند انجام دهند؟
- خطر مربوط به ویروس‌ها در چه جاهایی وجود دارد؟
- جلوگیری کردن از ویروس‌ها
- ویروس‌های سکتور بوت
- ویروس‌های انگلی
- ویروس‌های ماکرو (کلان دستور)

بخش دوم

- نرم‌افزار ضد ویروس
- پویشگرها
- Checksummer ها
- نرم‌افزارهای کاشف (Heuristic)
- هزینه‌های پنهانی ویروس‌ها
- ویروس‌نویسان چه کسانی هستند؟
- آیا نوشتن ویروس همیشه نادرست است؟
- ویروس‌های گول‌زن (Hoax ها)
- Hoax ها چیستند؟
- چرا Hoax ها یک معضل هستند؟
- چه کارهایی را در مورد Hoax ها می‌توان انجام داد؟
- تاریخچه مختصری از ویروس‌ها
- ۱۰ ویروس برتر

بخش سوم

- پست الکترونیک
- آیا به صرف خواندن نامه، ویروسی می‌شویم؟
- ویروس‌هایی که بطور خودکار از طریق نامه‌ها گسترش می‌یابند
- خطرات فایل‌های پیوندی
- چگونه ویروس‌های پستی را متوقف کنیم؟
- اینترنت
- کلیک کردن و آلوده شدن؟
- آیا به صرف دیدن وب‌سایت‌ها، ویروسی می‌شویم؟
- دستورات برنامه‌نویسی وب‌سایت‌ها
- اسب‌های تروای «در پشتی» و اینترنت
- آیا کوکی‌ها خطرناک هستند؟
- حمله‌ها به سوی وب‌سرورها
- امنیت در شبکه

بخش چهارم

- تلفن‌های موبایل و کامپیوترهای کف‌دستی
- آیا ویروس‌های موبایل هم وجود دارند؟
- تلفن‌های WAP و ویروس‌ها
- خطرات آتی برای WAP
- سیستم‌عامل‌های کامپیوترهای کف‌دستی
- ویروس‌ها برای یخچال‌ها؟
- چگونگی محافظت از ابزارهای متحرک (Mobile)
- ده مرحله برای ایجاد امنیت در کار با کامپیوتر
- لینک‌های مفید

بخش دوم

نرم‌افزار ضد ویروس

نرم‌افزار ضد ویروس می‌تواند ویروس‌ها را شناسایی کرده، از دسترسی به فایل‌های آلوده جلوگیری کند و در اغلب اوقات باعث حذف آلودگی‌ها شود. در اینجا مقدمه‌ای بر انواع مختلف نرم‌افزارهای موجود آورده می‌شود.

پویشگرها

پویشگرهای ویروس می‌توانند ویروس‌های مربوط به زمان خود را شناسایی کرده و اغلب آنها را از بین ببرند. بدون شک پویشگرها متداولترین انواع نرم‌افزارهای ضد ویروس می‌باشند، اما برای شناخت ویروس‌های جدید باید آنها را مرتبا Update کرد.

نحوه کارکرد پویشگرها به دو نوع دسترسی فعال (On access) و دسترسی زمان نیاز (On demand) تقسیم می‌شود. اکثر بسته‌های نرم‌افزاری ضد ویروس هر دو نوع را در خود دارند.

پویشگرهای با دسترسی فعال : هنگامی که آنها را اجرا کنید، بر روی دستگاه شما فعال می‌مانند. آنها فایل‌هایی را که شما قصد باز کردن یا اجرای آنها را دارید، بررسی می‌کنند.

پویشگرهای با دسترسی زمان نیاز: به شما این امکان را می‌دهند تا پویشی از درایوها یا فایل‌ها انجام داده و یا اینکه انجام عمل پویش را زمانبندی کنید.

Checksummer ها

Checksummer ها برنامه‌هایی هستند که می‌توانند زمان تغییر فایل‌ها را برای شما مشخص کنند. اگر ویروسی، برنامه یا سندی را آلوده کند – این کار سبب ایجاد تغییر در فایل یا برنامه در طی پروسه آلوده سازی می‌شود – در اینصورت برنامه Checksummer باید تغییرات را در گزارش خود بیاورد.

نکته مثبت در مورد این برنامه‌ها آن است که آنها مانند نرم‌افزارهای ضد ویروس که برای تشخیص وجود ویروس نیاز به دانستن همه چیز در باره همه ویروس‌ها دارند، نیازی

بـه دانسـتن ایـن اطلاعـات ندارنـد. بنابراین احتیاجی نیست که آنها را بطور مداوم Update کنیم.

نکـته منفـی در مورد این برنامه‌ها آن است که آنها نمی‌توانند بین تغییرات معمولی (مجـاز) بوجـود آمـده در یـک فایل و تغییرات بوجود آمده توسط یک ویروس تفاوتی قائل شـوند، بنابرایـن در هـر دو صـورت بـه کاربر هشدار می‌دهند. Checksummer ها در مورد اسنادی که بطور مداوم در حال تغییر هستند دارای مشکلات مشخصی می‌باشند.

بـه عـلاوه، آنها تنها زمانی به شما هشدار می‌دهند که فایل دچار آلودگی شده است. این برنامه‌ها نمی‌توانند ویروس را شناسایی کرده و یا باعث از بین رفتن آن شوند.

نرم‌افزارهای کاشف (Heuristic)

نـرم‌افزار کاشف با استفاده از قوانینی عمومی که در مورد ویروس‌ها و عملکردشان صـادق اسـت، سعی در شناخت همه ویروس‌ها اعم از ویروس‌های شناخته‌شده و ناشناس دارند. برخلاف نرم‌افزارهای پویشگر متداول، آنها نیازی به Update های مداوم برای آشنایی بـا تمـام ویروس‌های شناخته شده ندارند. با این حال، هنگامی که نوعی جدید از ویروس با عملکرد و ساختاری متفاوت از تمام ویروس‌های قبلی پدیدار می‌شود، نرم‌افزار کاشف آن را نخواهد شناخت و به Update شدن یا تعویض با نسخه جدیدتر نیازمند خواهد بود.

و در نهایت اینکه این نرم‌افزارها می‌توانند باعث ایجاد هشدارهای نادرست شوند.

هزینه‌های پنهانی ویروس‌ها

عملکرد ویروس‌ها تنها به صدمه زدن و پاک کردن اطلاعات محدود نمی‌شود بلکه آنها می‌توانند از راههای بسیار مخفی باعث صدمه زدن به حرفه و شغل شما شوند.

هر فردی راجع به ویروس‌ها می‌داند که آنها می‌توانند هر چیزی را بر روی دیسک‌ها پاک کنند یا به اسناد صدمه وارد کنند. چنین تاثیراتی جدی و مهم هستند اما می‌توان از راههایی مانند پشتیبان گیری به موقع و مناسب از اطلاعات و ... به سرعت اطلاعات را بازگردانده و باعث نجات آنها شد. خطرات بسیار جدی‌تر در تاثیرات جانبی و مخفی ویروس‌ها می‌باشد.

برای مثال ویروس‌ها می‌توانند از کار کردن کامپیوترها جلوگیری کرده و یا شما را مجبور کنند تا شبکه‌ای را تعطیل کنید. در خلال این مدت، ساعات مفید کاری و همچنین درآمدهای بسیاری از دست خواهد رفت.

بعضی ویروس‌ها باعث ایجاد اختلال در شغل‌های ارتباطی که طبیعتا وابستگی زیادی به ارتباطات دارند می‌شوند. ویروس‌های Melissa یا ExplorerZip که از طریق نامه‌های الکترونیکی گسترش می‌یابند، می‌توانند باعث تولید نامه‌های انبوه شوند بطوریکه سرورها را از کار بیاندازند. حتی در صورتیکه این اتفاق هم رخ ندهد، اغلب شرکتها در واکنش به چنین خطری، در هر صورت سرورهای پست الکترونیک خود را از فعالیت باز می‌دارند.

گذشته از موارد فوق، خطری هم در مورد محرمانه ماندن اطلاعات وجود دارد. ویروس Melissa می‌تواند اسناد شما را برای افرادی که نام آنها در دفترچه آدرس شما وجود دارد، ارسال کند در حالیکه ممکن است این اسناد، اطلاعات بسیار محرمانه‌ای را در خود داشته باشند.

ویروس‌ها همچنین می‌توانند اعتبار شما را بصورتی بسیار جدی در معرض خطر قرار دهند. اگر شما اسناد آلوده‌ای را برای مشتریان خود ارسال کنید، ممکن است آنها در مشارکت و تجارت با شما یا سازمان متبوعتان تجدید نظر کنند. بعضی اوقات هم ویروس‌ها خطر شرمندگی برای شما بوجود می‌آورند که کمتر از خطر آسیب به نام و آوازه تجاری شما نیست. برای مثال ویروس WM/Polypost کپی‌هایی از اسناد شما را با نام شما در یک شبکه خبری مربوط به گروههای نامشروع جنسی (Sex) قرار می‌دهد.

ویروس‌نویسان چه کسانی هستند؟

در صورتیکه کامپیوتر یا شبکه شما توسط ویروسی مورد صدمه قرار گیرد، شاید اولین چیزی که شما به زبان بیاورید – در کنار فحش و بد و بیراه! – این باشد که «چرا افراد این ویروس‌ها را می‌نویسند؟»

در اولین برداشت اینطور به نظر می‌رسد که نوشتن ویروس به انگیزه و محرک زیادی نیاز ندارد. نویسندگان ویروس از کار خود سودی چه از نظر مالی و چه از نظر رتبه‌های شغلی ندارند. آنها به ندرت به شهرت و آوازه‌های واقعی می‌رسند و برخلاف هکرها قربانیان مشخصی برای خود ندارند، چرا که ویروس‌ها بطور کاملا فراگیر و بدون هیچ تبعیضی! همه‌جا را فرا می‌گیرند.

علت ویروس‌نویسی بسیار قابل فهم خواهد بود اگر شما آن را به شکل‌هایی از شرارت! مانند ویرانگری و غارت در دنیای واقعی تشبیه کنید.

ویروس نویس‌ها اکثرا مذکر، مجرد و دارای سنی کمتر از ۲۵ سال هستند. احترام واعتبار آنها محدود به تصویب و موافقت رسمی گروههای همتایشان و یا حداقل یک انجمن کوچک الکترونیک می‌باشد. میزان تخریب و استثمار در نوشتن ویروس‌ها، یکی از کارهایی است که باعث ترقی رتبه نویسنده ویروس می‌شود.

ویروس‌ها همچنین نویسندگان خود را در دنیای ماشینی دارای قدرتی می‌کنند که آنها هیچ وقت امیدی به کسب آن قدرت در دنیای واقعی نخواهند داشت و به همین دلیل است که ویروس‌نویسان نام‌هایی برای خود انتخاب می‌کنند که توسط گروههای موسیقی Heavy Metal و گروههای ادبیات تخیلی برای نامیدن قهرمانان خیالی مورد استفاده قرار می‌گیرد.

آیا نوشتن ویروس همیشه نادرست است؟

اکثر ما به این مطلب اذعان داریم که ویروس‌ها چیزهای بدی هستند، اما آیا این نظر همیشه صحیح است؟

بسیاری از ویروس‌ها بی‌زیان بوده و یا اینکه فقط در حد یک شوخی می‌باشند. بقیه هم می‌توانند هشداری برای شکاف‌های امنیتی نرم‌افزارهای ما باشند. حتی بعضی افراد استدلال می‌کنند که ویروس‌ها می‌توانند مفید باشند، مثلا می‌توانند باعث شوند تا اشکالات نرم‌افزاری مورد تصحیح قرار گیرند. متاسفانه با توجه به دلایل زیر نظریه «بی‌زیان» بودن ویروس‌ها را نمی‌توان با مقوله امنیت جمع کرد.

دلیل اول اینکه ویروس‌ها بدون رضایت کاربران و در اغلب اوقات بدون آگاهی آنان تغییراتی را در کامپیوترهای آنها ایجاد می‌کنند. اینکار صرف‌نظر از خوب یا بد بودن قصد ویروس، غیر اخلاقی - و در بسیاری از کشورها غیر قانونی - می‌باشد. شما حق دخالت و فضولی در کامپیوتر فرد دیگری را ندارید، همانطور که نمی‌توانید بدون اینکه به کسی بگویی ماشین او را قرض! بگیرید (حتی اگر قصد شما تعویض روغن موتور ماشین او بوده باشد).

دلیل دوم آن است که ویروس‌ها همیشه کاری را که نویسنده آنها می‌خواسته، انجام نمی‌دهند. در صورتیکه ویروسی نادرست نوشته شده باشد، می‌تواند مشکلات ناخواسته‌ای را ایجاد کند. حتی اگر ویروسی بر روی سیستم‌عاملی که مورد نظرش بوده، مضر نباشد ممکن است بر روی سیستم‌عامل‌ها و یا برنامه‌های دیگر اثرات تخریبی بالایی داشته و یا اینکه نسخه‌های بعدی همان برنامه‌ها را در آینده با مشکل مواجه کند.

ویروس‌های اثبات عقاید

گاهی اوقات افراد ویروس‌هایی را می‌نویسند تا اثبات کنند که هنوز هم امکان بوجود آوردن نوعی جدید از ویروس‌ها وجود دارد. این ویروس‌ها تحت عنوان ویروس‌های «اثبات عقاید» شناخته می‌شوند. آنها معمولا تاثیرات جانبی نداشته و به کامپیوترهای کاربران معمولی کاری ندارند.

پژوهش؟

ویروس‌نویسان دوست دارند که کار خود را نوعی پژوهش معرفی کنند، اما از آنجایی که ویروس‌ها اغلب بسیار ناسالم نوشته می‌شوند و بطور تصادفی بر روی دستگاه کاربران خوش خیال آزاد می‌شوند و در نتیجه راهی برای جمع‌آوری نتایج آنها وجود ندارد، به سختی می‌توان کار ویروس‌نویسان را نوعی تحقیق و پژوهش قلمداد کرد.

ویروس‌های گول‌زن (Hoax ها)

اگر شما با جمله‌هایی مانند :

Good Times ، Budweiser Frogs یا How to give a cat a colonic متوجه وجود ویروسی شده‌اید، باید بدانید که قربانی یک Hoax شده‌اید. ویروس‌های Hoax و مخصوصا Hoaxهای پست الکترونیک، بسیار معمول بوده و می‌توانند مانند هر چیز دیگری از نظر زمانی و مالی پرهزینه باشند.

Hoax ها چیستند؟

Hoax ها گزارش‌هایی هستند از ویروس‌هایی که وجود ندارند! نوعا نامه‌هایی الکترونیکی وجود دارند که بعضی یا همه کارهایی که در زیر، لیست شده‌اند را انجام می‌دهند.

- هشدار به شما مبنی بر وجود ویروسی جدید با درجه تخریب بالا و غیرقابل شناسایی
- درخواست از شما برای اجتناب از خواندن نامه‌هایی که در موضوع آن‌ها عبارات مشخصی مانند Join the Crew یا Budweiser Frogs یا ... آمده است.
- مدعی شدن این مطلب که هشدار، توسط یک شرکت مهم نرم‌افزاری، موسسه تهیه کننده خدمات اینترنتی یا آژانسی دولتی و یا ... (مانند IBM ، Microsoft ، AOL، FCC یا ...) صادر شده است.
- ادعای اینکه ویروسی جدید می‌تواند کارهایی بعید انجام دهد. مثلا ویروس moment of silence ادعا می‌کرد که برای آلوده شدن یک کامپیوتر جدید نیازی به تبادل هیچ برنامه‌ای نیست (کامپیوتر خود به خود ویروسی می‌شود!).
- استفاده از حرف‌های بی‌معنی فنی برای توضیح دادن تاثیرات یک ویروس، مانند ویروس Good Times که می‌گفت «ویروس می‌تواند پردازنده کامپیوترهای شخصی را در یک حلقه دودویی بیکران با درجه پیچیدگی n گرفتار کند!».
- اصرار بر اینکه شما هشدارها را برای کاربران دیگر هم ارسال کنید.

Hoax ای که Hoax نیست.

در اول آوریل سال ۲۰۰۰ نامه‌ای با عنوان Rush-Killer virus alert انتشار یافت. این نامه در مورد ویروس‌هایی هشدار می‌داد که مودم را در اختیار گرفته و با شماره ۹۱۱ (شماره اورژانس آمریکا) تماس می‌گیرند. سپس در ادامه نامه از شما خواسته می‌شد تا این

نامـه را برای دیگران هم ارسال کنید. این نامه تمام نشانه‌های یک Hoax – که در قسمت قبلی به آنها اشاره شد – را در خود داشت، اما وجود ویروس هم حقیقت داشت. ویروس مورد نظر ویروسـی از نـوع BAT/911 بـود کـه از طـریق بـه اشتراک گذاشته شده‌های سیستم عامل ویندوز گسترش پیدا کرده و با شماره ۹۱۱ تماس برقرار می‌کرد.

تشـخیص یـک Hoax از پـیغام واقعی دشوار است. شما می‌توانید راهنمایی‌های ذکر شده در بخش «چه کارهایی را در مورد Hoax ها می‌توان انجام داد؟» در انتهای همین قسمت را مطالعه بفرمایید.

چرا Hoax ها یک معضل هستند؟

Hoax ها می‌توانند به اندازه یک ویروس واقعی مزاحم و پرهزینه باشند.

اگـر کاربـران بخواهـند یـک هشدار Hoax را به همه دوستان و همکاران خود ارسال کنـند، سـیلی بزرگ از نامه‌های الکترونیکی به راه خواهد افتاد. این کار می‌تواند باعث تراکم بـار سـرورهای پسـت الکترونـیک شـده و آنها را از کار بیاندازد. تاثیر این کار مانند تاثیر ویـروس واقعـی Love Bug اسـت بـا ایـن تفـاوت که فرستنده Hoax نیازی به نوشتن هیچ برنامه کامپیوتری نداشته است.

تنها کاربران شخصی نیستند که بیخود احساساتی شده و به Hoax ها واکنش نشان مـی‌دهـند. شـرکت‌هایـی که Hoax ها را دریافت می‌کنند، اغلب اقدامات شدیدی مانند تعطیل کردن شبکه یا سرور پست الکترونیک انجام می‌دهند. تاثیر فلج شدن چنین ارتباطاتی بسیار بیشـتر از تاثـیر بسـیاری از ویروس‌های واقعی خواهد بود و می‌تواند موجب جلوگیری از دسترسی به نامه‌هایی شود که ممکن است بسیار مهم باشند.

همچنین هشدارهای نادرست می‌توانند باعث شوند تا کوشش‌های در جهت مقابله با تهدیدات ویروس‌های واقعی کمتر و کمرنگ‌تر شود.

Hoax هـا مـی‌توانـند بطـور قـابل توجهـی پایدار بمانند، چرا که ویروس نیستند و نرم‌افزار ضد ویروس شما قادر به شناسایی و ناتوان کردن آنها نخواهد بود.

کدام یک زودتر آمد؟

یک Hoax می‌تواند موجب تهدیدی مانند تهدید یک ویروس واقعی شود و بالعکس. به مطلب زیر دقت کنید :

بعـد از آنکـه Good Times کـه یـک Hoax بـود در صـدر اخـبار قـرار گرفت، بعضی ویـروس نویسـان منتظر ماندند تا راز آن برای همه افشا شود، سپس یک ویروس واقعی با

همـان نـام نوشـتند (نویسـندگان نرم‌افزارهای ضد ویروس نام GT-Spoof را برای اینگونه ویروس‌ها برگزیده‌اند).

چه کارهایی را در مورد Hoax ها می‌توان انجام داد؟

وجـود Hoax هـا هـم مانـند ویروس‌ها یا نامه‌های زنجیره‌ای به قدرت گسترششان وابسـته است. اگر شما بتوانید کاربران را به شکستن زنجیره ارسال هشدارها متقاعد کنید، باعث محدود کردن زیان‌ها خواهید شد.

اتخاذ سیاستی برای شرکت در برابر هشدارهای ویروسی

یـک راه‌حـل ممکـن اسـت اتخاذ سیاستی برای شرکت در برابر هشدارهای ویروسی باشد. مثالی می‌آوریم:

«هیچ یک از هشدارهای در مورد ویروس، از هر نوعی را برای هیچ‌کس مگر شخص مسـؤول خدمـات ضـد ویروسـی ارسـال نکنـید. مهـم نیست که هشدار از طرف یک شرکت فروشـنده نـرم‌افـزارهای ضد ویروس آمده باشد یا اینکه اخطاری باشد از جانب یک شرکت بـزرگ کامپیوتری و یا اصلا پیغامی باشد از بهترین دوست شما. تمام هشدارهای ویروسی فقـط بـاید بـرای ... (نام شخص مسؤول خدمات ضد ویروسی) ارسال شود. فقط وظیفه این فـرد اسـت کـه بـه افراد دیگر برای هشدارهای ویروسی اخطار دهد. هر هشداری مربوط به ویروس که از هر منبع دیگری صادر شده باشد باید نادیده گرفته شود.»

تـا وقتـی کـه کاربـران از سیاست فوق پیروی کنند، هیچگاه سیلی از نامه‌ها به راه نخواهد افتاد و فقط کارشناس شرکت در مورد تهدیدات واقعی تصمیم خواهد گرفت.

آگاهی مداوم درباره Hoax ها

روش دیگـر آگاهی داشتن مداوم از Hoax ها با مطالعه صفحه‌های مربوط به آنها در وب‌سایت‌های مرتبط مانند آدرس www.sophos.com/virusinfo/hoaxes می‌باشد.

تاریخچه مختصری از ویروس‌ها

۱۹۵۰ : لابراتوارهای Bell نسخه‌ای نمایشی از یک بازی را طراحی کردند که در آن، هـر یک از بازیکنان می‌توانست از برنامه‌هایی مخرب برای حمله به کامپیوترهای افراد دیگر استفاده کند.

۱۹۷۵ : آقـای John Brunner نویسـنده داستان‌های عملی-تخیلی، داستانی درباره کرمی کامپیوتری نوشت که در تمام شبکه‌ها گسترش پیدا می‌کرد.

۱۹۸۴ : برای اولین بار نام «ویروس کامپیوتری» - توسط آقای Fred Cohen در یک مقاله - برای برنامه‌های مخرب بکار برده شد.

۱۹۸۶ : دو بـرادر پاکسـتانی، اولین ویروس کامپیوتری با نام Brain را برای احقاق حقوق خود بوجود آوردند.

۱۹۸۷ : کـرم اینترنتـی «درخت کریسمس (Christmas tree)» شبکه جهان‌گستر IBM را فلج کرد.

۱۹۸۸ : کرمی با نام «کرم اینترنت (Internet Worm)» شبکه اینترنت US DARPA را درنوردید.

۱۹۹۲ : گـرچه کامپـیوترهای بسـیار کمی آلوده شدند، اما هراسی شدید از ویروس «میکلانژ (Michelangelo)» جهان را فرا گرفت.

۱۹۹۴ : «اوقات خوش (Good Times)»، اولین ویروس Hoax مهم، پدیدار شد.

۱۹۹۵ : اولین ویروس از نوع ماکرو با نام Concept بوجود آمد.

۱۹۹۸ : ویـروس CIH یـا همـان Chernobyl ، اولیـن ویروسـی شـد که توانست به سخت‌افزار کامپیوتر صدمه بزند.

۱۹۹۹ : Melissa ، ویروسی که خود را به کمک نامه‌های الکترونیکی پیش می‌برد، در سطح جهان گسترش پیدا کرد.

همچنیـن BubbleBoy به عنوان اولین ویروسی که فقط با مشاهده نامه الکترونیکی، کامپیوتر را آلوده می‌کرد، ظاهر شد.

۲۰۰۰ : ویروس Love Bug هنوز هم موفق‌ترین ویروس پستی می‌باشد.

همچنیـن در ایـن تـاریخ اولیـن ویـروس بـرای سیسـتم‌عـامل‌هـای کامپـیوترهای کف‌دستی ظاهر شد، اگرچه هیچ کاربری قربانی آن نشد.

۲۰۰۱ : ویروسـی کـه ادعا می‌کرد تصاویری از بازیکن تنیس «Anna Kournikova» را در خود دارد، صدها هزار کامپیوتر را در سراسر جهان آلوده کرد.

۲۰۰۲ : آقای David L Smith ، نویسنده ویروس Melissa توسط دادگاهی در آمریکا به ۲۰ ماه زندان محکوم شد.

۲۰۰۳ : جامعـه امنیت کامپیوتر، دانشگاه Calgary را به خاطر اعلام اینکه قصد دارد تا رشته ویروس نویسی را برای دانشجویان دایر کند، محکوم کرد.

۱۰ ویروس برتر

کدامیک از ویروس‌ها تابحال بیشترین موفقیت را داشته‌اند؟ در این قسمت گزیده‌ای از ویروس‌هایی آورده می‌شود که توانسته‌اند:

به دورترین نقاط انتقال پیدا کنند،

بیشترین تعداد کامپیوتر را آلوده کنند،

و یا اینکه بیشترین طول عمر را داشته باشند.

ویروس Love Bug (VBS/LoveLet-A)

احتمالا ویروس Love Bug بهترین ویروس شناخته شده می‌باشد. این ویروس با تظاهر خود به عنوان یک نامه عاشقانه و برانگیختن حس کنجکاوی کاربران، در ساعاتی توانست در نقاط مختلف جهان گسترش پیدا کند.

اولین مشاهده : ماه می از سال ۲۰۰۰

سرچشمه : فیلیپین

شهرت : نامه عاشقانه

نوع : کرم اسکریپتی ویژوال بیسیک

راه اندازی ویروس : در اولین آلودگی

تاثیرات : نسخه اصلی این ویروس نامه‌ای با عنوان «دوستت دارم» با متن «در کمال لطف و مهربانی، نامه‌ای عاشقانه از من به تو، پیوند این نامه شده است، آن را بخوان» را برای کاربران می‌فرستد. باز کردن فایل پیوندی، باعث راه‌اندازی ویروس خواهد شد. در صورتیکه برنامه Outlook شرکت مایکروسافت نصب شده باشد، ویروس سعی خواهد کرد تا خود را به آدرس تمام افرادی که آدرس آنها در دفترچه آدرس برنامه Outlook وجود دارد، ارسال کند. این ویروس همچنین می‌تواند خود را در گروههای خبری توزیع کرده، اطلاعات کاربران را مورد سرقت قرار دهد و فایل‌های بخصوصی را بازنویسی کند.

ویروس FORM

نام ویروس Form به خاطر گسترش هشت ساله آن – که هنوز هم ادامه دارد – در لیست ۱۰ ویروس برتر آورده شده است. در سیستم عامل DOS و نسخه‌های ابتدایی ویندوز، این ویروس بسیار مخفی عمل کرده و به همین خاطر توانسته در ابعادی وسیع گسترش پیدا کند.

اولین مشاهده : سال ۱۹۹۱

سرچشمه : سوئیس

نوع : ویروس سکتور بوت

راه اندازی ویروس : در روز ۱۸ ماه

تاثیرات : هنگامی که شما هر دکمه‌ای بر روی صفحه کلید را فشار دهید، این ویروس باعث تولید یک کلیک خواهد شد. می‌تواند باعث عدم فعالیت کامپیوترهای مبتنی بر سیستم عامل NT شود.

کرم Kakworm (VBS/Kakworm)

این کرم فقط با خواندن نامه آلوده، باعث آلوده شدن دستگاه کاربر می‌شود.

اولین مشاهده : سال ۱۹۹۹

نوع : کرم اسکریپتی ویژوال بیسیک

راه اندازی ویروس : در بیشتر موارد آلودگی، آلودگی با اولین اجرای ویروس شروع شده که این نوع آلودگی بیشترین آلودگی از این ویروس را داشته و در نوع دیگر، ویروس در روز اول هر ماه فعال می‌شود که این نوع با فعالیت جانبی Shut Down کردن ویندوز همراه است.

تاثیرات : این کرم در پیامی که از طریق پست الکترونیک دریافت می‌شود، جاسازی شده است. در صورتی که شما از برنامه Outlook یا Outlook Express به همراه Internet Explorer 5 استفاده می‌کنید، ممکن است کامپیوترتان به هنگام باز کردن یا مشاهده نامه آلوده، ویروسی شود. این ویروس تنظیمات برنامه Outlook Express را چنان تغییر می‌دهد که با هر نامه فرستاده شده از طرف شما، دستورات ویروسی هم به طور اتوماتیک فرستاده می‌شوند. در روز اول هر ماه، بعد از ساعت ۵ بعدازظهر، ویروس پیغام Kagou_Anti_kro$oft says not today را نمایش داده و سیستم‌عامل ویندوز را خاموش می‌کند.

ویروس Anticmos

ویروسی بخصوص از نوع ویروس سکتور بوت است. در اواسط دهه ۱۹۹۰ شروع به گسترش کرده و به طور متناوب در لیست ۱۰ ویروس برتر قرار گرفته است.

اولین مشاهده : ماه ژانویه از سال ۱۹۹۴

سرچشمه : اولین شناسایی در هنگ‌کنگ بوده اما عقیده بر آن است که سرچشمه آن کشور چین می‌باشد.

نوع : ویروس سکتور بوت

راه اندازی ویروس : تصادفی

تاثیرات : سعی در پاک کردن اطلاعات مربوط به درایورهای نصب شده فلاپی و دیسک سخت.

ویروس Melissa (WM97/Melissa)

ملیسا ویروسی از نوع ویروس های پست الکترونیکی بوده و از ظرافت‌های روانشناختی برای گسترش سریع استفاده می‌کند. این ویروس اینطور وانمود می‌کند که از طرف فردی آشنا برای شما آمده و شامل متنی است که شما حتما می‌خواهید آن را بخوانید. در نتیجه به همین سادگی ویروس ملیسا سرتاسر دنیا را تنها در یک روز می‌پیماید.

اولین مشاهده : ماه مارس از سال ۱۹۹۹

سرچشمه : آقای David L Smith ، برنامه‌نویس ۳۱ ساله آمریکایی که متنی آلوده به ویروس را در گروههای خبری وابسته به گروههای نامشروع جنسی (Sex) قرار داده بود.

نوع : ویروس ماکرو مربوط به برنامه‌های Word 97 و Word 2000

راه اندازی ویروس : در اولین اجرا

تاثیرات : با تهیه یک نامه که در موضوع آن، نام کاربر استفاده کننده از کامپیوتر آورده شده و ارسال آن نامه به پنجاه آدرس اول از تمام کتابچه آدرس‌هایی که در دسترس برنامه Microsoft Outlook باشند، خود را گسترش می‌دهد. نامه فرستاده شده شامل فایلی پیوندی است که نسخه‌ای از متنی آلوده به ویروس را در خود دارد. در صورتیکه در زمان و تاریخ باز شدن فایل، دقیقه و شماره روز یکی باشند (مثلا ساعت ۰۵ : ۱۰ از روز پنجم ماه)، ویروس متنی راجع به بازی Scrabble را به فایل اضافه خواهد کرد.

ویروس New Zealand

بدون شک در اوایل دهه ۱۹۹۰، این ویروس یکی از ویروس‌های فراگیر بوده است.

اولین مشاهده : اواخر دهه ۱۹۸۰

سرچشمه : نیوزیلند

شهرت : سنگ‌شده

نوع : ویروس سکتور بوت

راه اندازی ویروس : در صورتیکه سیستم از طریق فلاپی راه‌اندازی شود، در هر ۸ مرتبه، یکبار این ویروس فعال می‌شود.

تاثیرات : پیام «کامپیوتر شما در حال حاضر سنگ شده» را نمایش می‌دهد. این ویروس نسخه‌ای از سکتور بوت اصلی را در آخرین سکتور از فهرست ریشه یک دیسکت ۳۶۰ کیلوبایتی قرار می‌دهد. این کار می‌تواند به دیسکت‌های با حجم بیشتر صدمه بزند.

ویروس Concept (WM/Concept)

ویروس Concept که توانست تصادفا حامل مناسبی مانند نرم‌افزارهای Office شرکت مایکروسافت را بدست آورد، موفقیتی ناگهانی کسب کرد. این ویروس که اولین نوعی بود که به صورت ماکرو (کلان‌دستور) نوشته شده بود، به یکی از ویروس‌های فراگیر در سالهای ۱۹۹۶ تا ۱۹۹۸ تبدیل شد. ویروس Concept کنترل دستگاه را با اجرای ماکروی AutoOpen خود که برنامه Word آن را بصورت خودکار اجرا می‌کرد، بدست آورده و آلودگی را از طریق ماکروی FileSaveAs خود که در هر بار Save شدن فایلی در برنامه Word اجرا می‌شد، انتقال می‌داد. گونه‌های مختلفی از این ویروس وجود دارد.

اولین مشاهده : ماه آگوست از سال ۱۹۹۵

نوع : ویروس ماکرو

تاثیرات : هنگامی که شما سندی آلوده را باز می‌کنید، یک صفحه پیغام با عنوان Microsoft Word نمایان می‌شود. این ویروس شامل عبارت That's enough to prove my point بوده اما آن را هیچگاه نمایش نمی‌دهد.

ویروس CIH یا Chernobyl (W95/CIH-10xx)

CIH اولین ویروسی بود که توانست به سخت افزار کامپیوتر صدمه وارد کند. به محض اینکه این ویروس اطلاعات بایوس را بازنویسی کند، کامپیوتر دیگر قابل استفاده نخواهد بود مگر آنکه چیپ بایوس آن تعویض شود.

اولین مشاهده : ماه ژوئن از سال ۱۹۹۸

سرچشمه : نوشته شده توسط Chen Ing-Hau از تایوان

نوع : ویروسی انگلی که بر روی کامپیوترهای مبتنی بر سیستم‌عامل ویندوز ۹۵ اجرا می‌شود.

راه اندازی ویروس : در روز ۲۶ ماه آوریل. انواع دیگر آن در روزهای ۲۶ از ماه ژوئن و یا روز ۲۶ هر ماه آزاد می‌شوند.

تاثیرات : بازنویسی کردن اطلاعات روی بایوس و پس از آن اطلاعات بر روی دیسک سخت.

ویروس Parity Boot

این ویروس بر روی سکتور بوت فلاپی‌ها گسترش می‌یابد. موفقیت آن مؤید این مطلب است که ویروس‌های از نوع سکتور بوت – که در دهه ۱۹۸۰ و اوایل دهه ۱۹۹۰ فراگیر بوده‌اند – هنوز هم می‌توانند پررونق باشند.

نام این ویروس در اکثر گزارش‌های مربوط به سال ۱۹۹۸ قابل مشاهده می‌باشد. آلودگی فوق‌العاده این ویروس مربوط به کشور آلمان می‌باشد، جایی که توانست خود را از طریق دیسکت‌های توزیع شده به همراه یک مجله منتشر کند (در سال ۱۹۹۴).

اولین مشاهده : ماه مارس از سال ۱۹۹۳

سرچشمه : احتمالا کشور آلمان

نوع : ویروس سکتور بوت

راه اندازی ویروس : تصادفی

تاثیرات : پیغام PARITY CHECK را نمایش داده و باعث قفل شدن کامپیوتر می‌شود. این کار تقلیدی از رخداد یک خطای واقعی حافظه می‌باشد. در نتیجه، اغلب اوقات کاربران تصور می‌کنند که مشکلی در حافظه RAM دستگاه آنها وجود دارد.

ویروس Happy99 (W32/Ska-Happy99)

اولین ویروس شناخته شده‌ای بود که توانست به سرعت خود را از طریق پست الکترونیک گسترش دهد.

اولین مشاهده : ماه ژانویه از سال ۱۹۹۹

سرچشمه : توسط Spanska ویروس نویس فرانسوی به یک گروه خبری ارسال شد.

نوع : ویروس فایلی که بر روی سیستم‌عامل‌های ویندوز 95 ، 98 ، ME ، NT ، 2000 و XP اجرا می‌شود.

تاثیرات : نمایی از یک آتش بازی و سپس پیام «سال ۱۹۹۹ مبارک» را نمایش می‌دهد. این ویروس فایل wsock32.dll در شاخه System از سیستم‌عامل Windows را چنان تغییر می‌دهد که بعد از هر نامه‌ای که فرستاده می‌شود، پیام دیگری هم که شامل ویروس می‌باشد ارسال خواهد شد.