مجله تخصصی

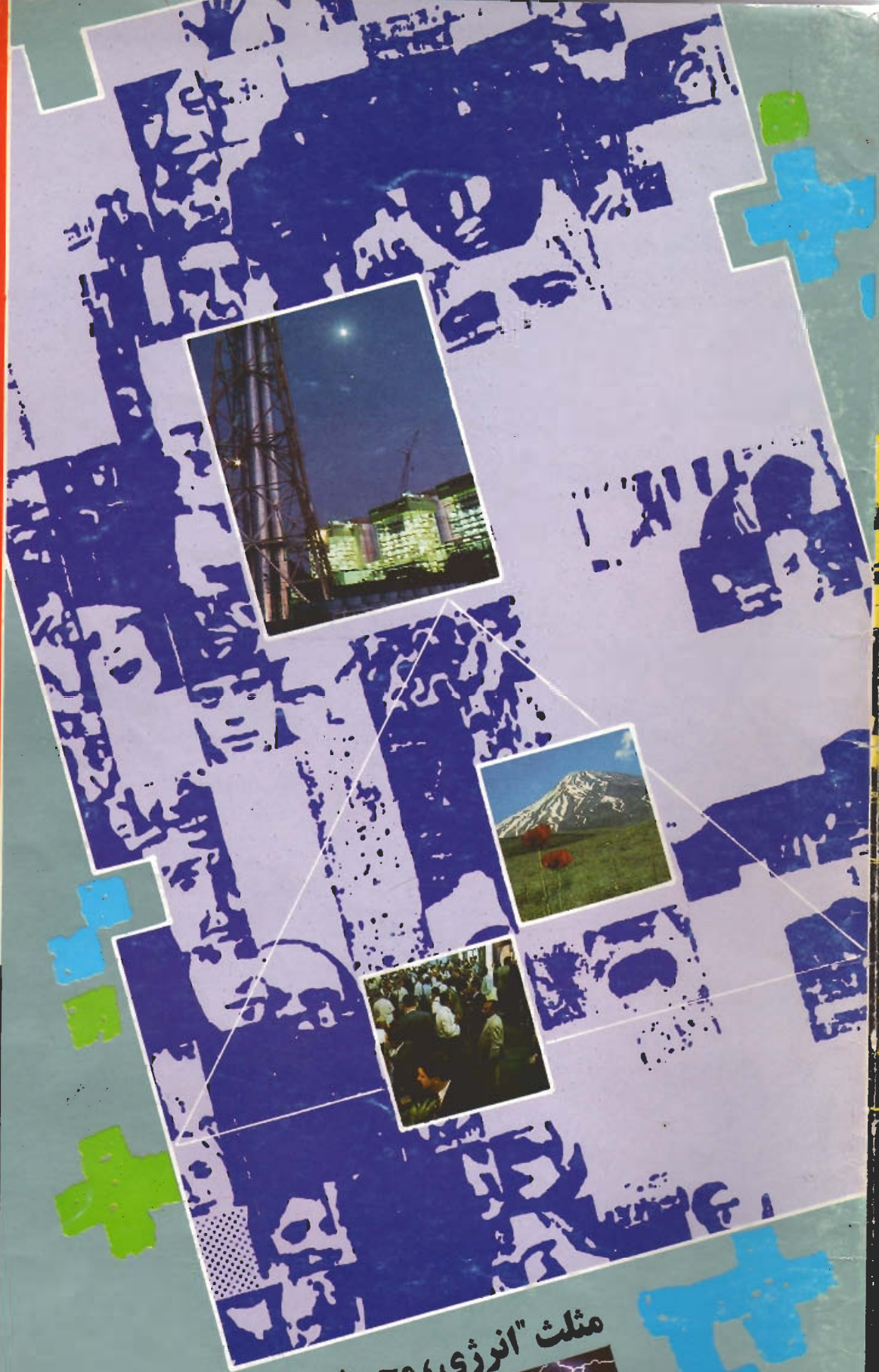
برق و الکترونیک

شماره اول، مهرماه ۱۳۷۳، قیمت ۵۰۰ ریال

ماهنامه انجمن مهندسین برق و الکترونیک ایران

○ دیدگاههای مشاور تحقیقاتی رئیس جمهوری در بارهٔ:

صنعت برق و جایگاه تحقیقات در کشور



مثلث "انرژی، محیط زیست، رشد جمعیت"

مشکل آینده جهان

برنامه های مخرب

نوشته : جان بولز و کولن پلاتز دانشگاه کارولینای جنوبی
ترجمه : ادیک باغداساریان
منبع : IEEE SPECTRUM AUGUST 1992

● اصطلاح "ویروس کامپیوتری" اغلب در معنی عمومی برای انوع مختلف برنامه های مخرب کامپیوتری به کار می‌رود اگر چه می‌توان ویروس را یکی از آنها دانست. بسیاری از برنامه‌های مخرب بی‌خطر هستند /اگر چه فضای دیسک و حافظه و زمان پردازنده را اشغال می‌کنند / مگر اینکه وضعیت خاصی ایجاد شود تا مشغول تخریب اطلاعات و نرم افزارهای سیستم شوند.

در ششم ماه مارس ۱۹۹۲ نوعی ویروس کامپیوتری موسوم به میکل‌آنژ با نوشتن تصادفی روی دیسک های سخت حدود ۲۰۰۰ کامپیوتر شخصی در سراسر جهان آسیب بسیاری به نرم‌افزارهای آنها وارد کرد. خسارت می‌توانست حتی بیش از آن باشد ، یک مرکز پژوهشی واقع در پرتلند ایالات متحده آمریکا چنین برآورد کرد که ۶۴۳۹۰ کامپیوتر در آن کشور به وسیلهٔ این ویروس آلوده شده بودند اما به لطف برنامه‌های ضد ویروس میکل آنژ، تنها به چند صد کامپیوتر آسیب وارد شد. به کاربران کامپیوترهای شخصی آموزش داده شده بود که از برنامه‌های ضد ویروس برای زدودن ویروس‌ها از سیستم‌های خود استفاده کنند و یا تاریخ کامپیوترهای خود را نسبت به

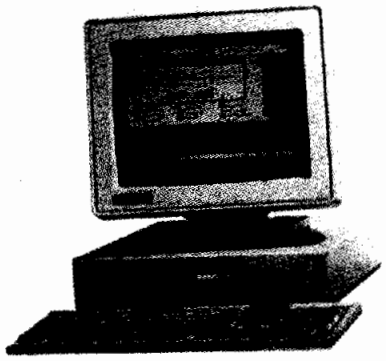
تاریخ ششم ماه مارس جلوتر ببرند تا از فعال شدن ویروس جلوگیری شود.

ویروس میکل آنژ نخستین بار در چهارم فوریه ۱۹۹۱ ظاهر شد، در یکی از فروشگاه‌های کامپیوتر واقع در حومه ملبورن استرالیا یکی از کامپیوترهای شخصی دچار مشکلی شد و پس از نصب برنامه‌ای به نام VET برای آمادگی جهت انتقال، به جای 640K تنها 639K حافظه اصلی مسوجود بود. آنگاه مشاهده شد که قطاع راه‌اندازی (Boot Sector) دیسک کاملاً پاک شده و تغییر کرده است. آزمایش‌های بیشتر وجود نوعی ویروس ناشناخته را نشان داد. چند روز بعد ماکس تفلر (Max Tefler) در انستیتو چیشورن ویکتوریای استرالیا از این ویروس که در ششم ماه مارس فعال شده بود آگاهی یافت این روز اتفاقاً روز تولد تفلر و میکل آنژ بوناروتی (Michelangelo Buonarroti) نقاش، حجار، معمار و شاعر ایتالیایی (۱۵۶۴ - ۱۴۷۵ م) بود بنابراین ویروس تازه کشف شده با نام این هنرمند بزرگ دوران رنسانس شناخته شد.

این ویروس که به وسیلهٔ فرد یا افراد ناشناس، پیشتر نوشته شده و انتشار یافته بود توسط دیسک های نرم (فلاپی) از سیستم‌های آلوده به کامپیوترهای دیگر سرایت کرد. شرکت‌های متعدد ناآگاهانه کامپیوترهای آلوده خود را توزیع می‌کردند از جمله شرکت اینتل در سانتاکلارای کالیفرنیا، ۸۳۹ نسخه از برنامه کمکی سرویس دهنده چاپ LAN Spool 3.01 را که آلوده به ویروس میکل آنژ بود پیش از کشف آن در اختیار مشتریان خود قرار داد. شرکت لیدینگ اج پرودواکتس در وستبوروی ماساچوست حدود ۵۰۰ کامپیوتر شخصی آلوده به این ویروس را به فروش رساند و شرکت لوتوس در کمبریج ماساچوست نیز تعدادی از نسخه‌های CD/Networker را پخش کرد. زمانی که مشکل مشاهده شد، اکثر شرکت‌ها برنامه‌های ضد ویروس برای مشتریان خود ارسال کردند و حتی شرکت لوتوس برای رفع این اشکال کارشناسان خود را به نزد مشتریان گسیل داشت.

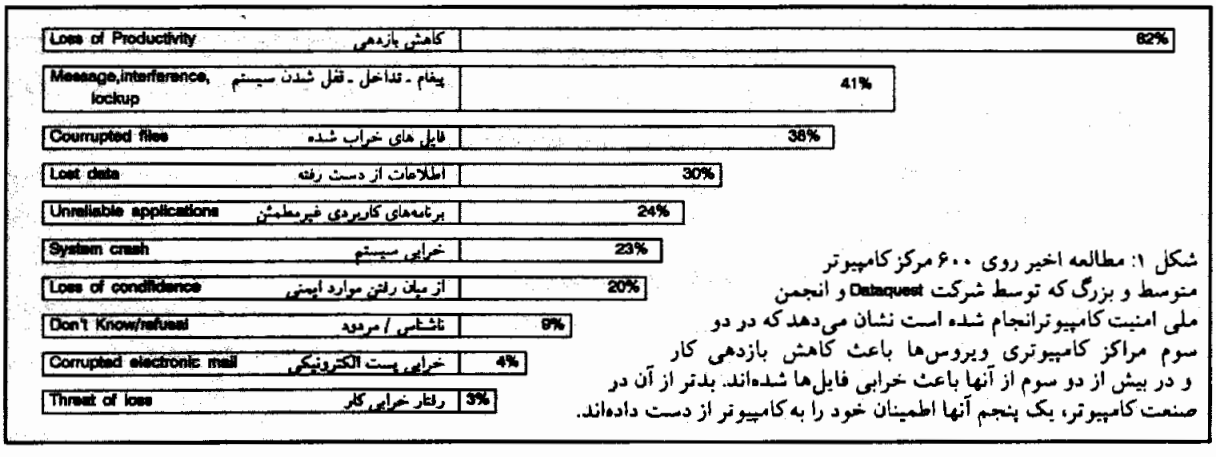
انوع برنامه‌های مخرب

میکل آنژ تنها یکی از ویروس‌های مخرب کامپیوتر است. پژوهش هایی که پیش از مقابله همه جانبه با میکل آنژ صورت گرفته‌اند نشان می‌دهند که نرم افزار مخرب تأثیر زیان آوری در سازماندهی به جا می‌گذارد. از دست رفتن بازدهی و اطلاعات بر اثر فعالیت ویروس‌ها بارها تجربه شده است. (شکل شماره ۱).

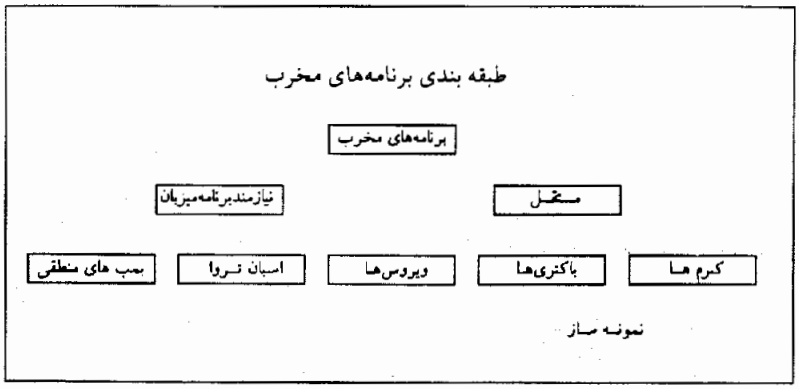


با توجه به نوع و روش دسته‌بندی می‌توان تعداد ویروس ها راکمتر از یک صد و یا بیش از هزار دانست. در مرکز آزمایش ویروس دانشگاه هامبورگ آلمان بیش از ۳۰۰ نوع ویروس مخرب کامپیوترهای شخصی آی بی ام شناسایی شده است. میکل آنژ نوعی ویروس موسوم به Stoned است که روی رکورد راه‌اندازی اصلی دیسک (Master Boot Record) اثر می‌گذارد.

اصطلاح "ویروس کامپیوتری" اغلب در معنی عمومی برای انوع مختلف برنامه های مخرب کامپیوتری به‌کار می‌رود اگر چه می‌توان ویروس را یکی از آنها دانست. (شکل شماره ۲). بسیاری از برنامه‌های مخرب بی‌خطر هستند /اگر چه فضای دیسک و حافظه و زمان پردازنده را اشغال می‌کنند/ مگر



شکل ۱: مطالعه اخیر روی ۶۰۰ مرکز کامپیوتر متوسط و بزرگ که توسط شرکت Dataquest و انجمن ملی امنیت کامپیوترانجام شده است نشان می‌دهد که در دو سوم مراکز کامپیوتری ویروس‌ها باعث کاهش بازدهی کار و در بیش از دو سوم از آنها باعث خرابی فایل‌ها شده‌اند. بدتر از آن در صنعت کامپیوتر، یک پنجم آنها اطمینان خود را به کامپیوتر از دست داده‌اند.



شکل شماره ۲: طبقه بندی برنامه‌های مخرب بر اساس عملکرد عمومی آنها تنظیم شده است . بمب های منطقی، اسبان تروا و ویروس‌ها در یک برنامه میزبان مستقر می‌شوند و تنها وقتی که این برنامه اجرا می‌شود فعال می‌شوند و موجودیت آنها به این برنامه بستگی دارد. باکتری‌ها و کرم‌ها به طور مستقل عمل می‌کنند. ویروس‌ها، باکتری‌ها و کرم ها نمونه سازی می‌کنند، در حالی که بمب‌های منطقی و اسبان تروا چنین نیستند

اینکه وضعیت خاصی ایجاد شود تا مشغول تخریب اطلاعات و نرم افزارهای سیستم شوند.

فعال شدن این برنامه‌ها در شرایط خاص روی می‌دهد مانند دسترسی به یک فایل اطلاعاتی خاص ، گذشت زمان مشخص و یا فرا رسیدن تاریخ خاص . خساراتی که معمولاً به وجود می‌آید شامل تخریب داده ها ، شبیه سازی مشکلات سخت افزاری ، ایجاد دسترسی غیرمجاز به سیستم و قفل شدن سیستم است .

اسبان تروا

ویروس های اسبان تروا چنان که از نامشان برمی‌آید در ابتدا که ظاهر می‌شوند بی‌زیان هستند. اینها اغلب عمل مفیدی انجام می‌دهند. اما کدهای مخفی داخل برنامه در کامپیوتر یکباره فعال می‌شوند و دست به عملیات تخریبی می‌زنند و یا امنیت دسترسی را از میان می‌برند و افراد غیرمجاز می‌توانند به سیستم و یا فایل‌های خاصی دسترسی یابند.

امکان نشاندن چنین کدی در یک برنامه ، بدون تغییر کد اصلی توسط کن تامپسون (Ken Thompson) آشکار شد که همراه با دنیس ریچی (Deninis Ritchie) سیستم [illegible] عامل یونیکس، را پدید آورد . او هنگام دریافت جایزه انجمن ابزارهای کامپیوتری (ACM) به خاطر مشارکت در طراحی یونیکس نشان داد که یک برنامه مترجم یا کمپایلر (Compiler) می‌تواند هنگام ترجمه یک برنامه زیان آور، اسب تروا ایجاد کند.

تامپسون می‌خواست فرمان Login /ابزار استاندارد دسترسی به سیستم‌های یونیکس/ را تغییر دهد تا کلمه رمز کاربر و یا یک کلمه رمز خاص را که خود مشخص می‌کند پذیرفته شود. او آنگاه می‌توانست کلمه رمز خاص خود را برای ورود به سیستم یونیکس به کار برد حتی به عنوان سرپرست می‌توانست به همه منابع سیستم دسترسی یابد.

```
Compile (s)
char *s;
{
 if (match (s,"pattern")
    {
      compile ("bug code");
      return;
    }
  < other statements ...>
```

شکل شماره ۳: با استفاده از این نوع روتین، کمپایلرها می‌توانند درکد منبع دنبال یک رشته کاراکتر بگردند و "کد مخرب" را به طور مخفیانه در آن درج کنند.

برنامه‌نویسان این وسیله دسترسی را یک "تله" قلمداد کردند.

او غیر از تغییر کد منبع فرمان Login /که به آسانی قابل دسترسی بود/ اقدام به تغییر کمپایلر C نیز کرد. زمانی که کمپایلر تغییر یافته برای ایجاد کد ماشین به کار رفت این برنامه مترجم می‌توانست تک تک سطرهای کد منبع را بررسی و برنامه Login را پیدا کند. کمپایلر سپس برنامه تامپسون را که برای ایجاد تله پدید آمده بود تغییر داد. (شکل شماره ۳) . حتی اگر نرم افزار ترجمه شده (کمپایل شده) شامل تله تامپسون می‌بود ، برنامه منبع فرمان Login تغییری نمی‌کرد بنابراین اثری از تغییرات نداشت .

حتی کد منبع خود کمپایلر نیازی به شمول کد منبع ورود اسب تروا در کد Login ندارد. کمپایلر C خود برنامه‌ای است که به زبان C نوشته شده و می‌باید توسط یک کمپایلر ترجمه شود . اگر کمپایلر اخیر شامل کد برنامه اسب تروا باشد ، به طور مداوم این کد را به کمپایلرهایی که ترجمه می‌کند انتقال می‌دهد بنابراین اسب تروا به کمپایلر بعدی انتقال می‌یابد و اگر کمپایلر اصلی تغییر یافته تخریب شده باشد کد برنامه مخرب در کد منبع هر برنامه دیگر وجود نخواهد داشت . تنها بررسی دقیق و کامل خروجی کمپایلر می‌تواند به کشف تغییرات منتهی شود.

ویروس ها

ویروس ها برنامه‌های کوچکی هستند که کد آنها کمتر از ۲ یا ۳ کیلوبایت است و خود را به سایر برنامه‌ها می‌چسبانند و معمولاً به عنوان چند دستورالعمل نخست برنامه میزبان ، اجرا می‌شوند. آنها در دو مرحله عمل می‌کنند : مرحله تکثیر که به تولید مثل ویروس می‌انجامد ولی هیچ اثر سوئی بر سیستم میزبان ندارد و

مرحله فعالیت تغییرات پدید می‌آید و غالباً سیستم کامپیوتر میزبان خسارت می‌بیند.

اکثر ویروس ها شامل یک رشته کاراکترند که به صورت یک نشانگذار (Marker) عمل می‌کند و آلودگی برنامه را نشان می‌دهد. هنگامی که ویروس تکثیر می‌شود به طور تصادفی فایل‌های اجرایی را انتخاب و وجود نشانگذار را در آنها بررسی می‌کند. اگر نشانگذار موجود باشد، فایل قبلاً آلوده شده است و ویروس یک فایل اجرایی دیگر را انتخاب می‌کند. هنگامی که ویروس برنامه غیرآلوده‌ای پیداکند یک نسخه از برنامه خود را در آن قرار می‌دهد. بدین سان ویروس از آلوده سازی مکرر و طولانی شدن فایل مقصد جلوگیری می‌کند و می‌تواند برنامه‌های بیشتری را بدون اشتغال زیاد و قابل توجه فضای دیسک، آلوده سازد.

ویروس در مرحله تکثیر، سعی می‌کند تا سرحد امکان برنامه‌های بیشتری را آلوده سازد. از آنجا که ویروس تنها هنگام اجرای برنامه آلوده شده می‌تواند خرابکاری کند، بنابراین آلوده کردن برنامه‌های بیشتر این امکان را فراهم می‌سازد که برنامه آلوده هنگام فراهم شدن شرط خاصی به اجرا درآید.

بخشی از کد ویروس بررسی می‌کند که آیا شرط خرابکاری تأمین شده است. اگر چنین باشد ویروس وارد مرحله فعالیت می‌شود در غیراین‌صورت کنترل به برنامه اصلی بازمی‌گردد. نمونه‌ای از این شرط ها می‌تواند تعداد دفعات اجرای یک برنامه و یا فرارسیدن تاریخ خاصی باشد (جمعه سیزدهم و روز اول آوریل یعنی روز دروغ و شوخی).

در مرحله فعالیت، بسیاری از ویروس‌ها نوعی دستکاری انجام می‌دهند که بیانگر وجودشان است. یک نوع دستکاری نمونه می‌تواند نمایش مطالب غیرمعمول و یا سرگرم کننده، راه اندازی مجدد سیستم، تغییر داده‌های عددی در برنامه‌های صفحه گسترده، پاک شدن صدای غیرمعمول، فایل ها و حتی قالب بندی مجدد دیسک سخت باشد.

● کاربران سیستم باید برای آگاهی بیشتر از روش حفاظت، آموزش لازم را ببینند. مطالعات اخیر نشان می‌دهد که اکثر ویروس‌ها توسط دیسک‌هایی که کاربران در سیستم قرار می‌دهند و یا به دیگران اجازه این کار را می‌دهند، منتقل می‌شوند.

سه ویژگی در معماری، کامپیوترهای شخصی آی بی ام و سازگار با آنها را به‌طور اخص نسبت به آلودگی ویروسی حساس و مستعد می‌سازد. نخست این که آنها فاقد سخت افزار ایمنی حافظه هستند و اجازه می‌دهند هر برنامه‌ای به تمام نقاط و منابع سیستم دسترسی یابد. دوم، سازگاری نرم افزاری DOS امکان می‌دهد یک برنامه در پیکربندی‌های مختلف و متعدد کامپیوتر اجرا شود. سوم، دسترسی و پیکربندی مجدد سیستم وقفه و سیستم ورود و خروج پایه (Bios) /که در حافظه تصادفی (RAM) ذخیره می‌شوند/ آسان است.

وقتی که اولی فعال شود، کامپیوتر وارد مراحل طولانی راه‌اندازی، آزمایش خود و انتقال کنترل بین روتین‌های آغازگری سیستم می‌شود. اگر چه اکثر این روتین ها در حافظه فقط خواندنی (ROM) ذخیره می‌شوند و در مقابل ویروس‌ها مصون هستند، اطلاعات برداری و تنظیم پارامترها توسط سیستم در حافظه تصادفی (RAM) ذخیره می‌شود. ویروس ها می‌توانند از این امر برای تکثیر خود استفاده کنند.

هنگامی که یک دیسک به صورت قابل راه‌اندازی قالب بندی می‌شود، قطاع اول معروف به رکورد راه‌اندازی اصلی (Master Boot Record = MBR) بلوک پارامترهای BIOS (BPB) را که شامل اطلاعات مفصل جابجایی سیستم فایل روی دیسک (جدول تخصیصی جای فایل‌ها یا FAT) و دستورالعمل‌هایی برای آغاز ردیف راه‌اندازی سیستم (System Boot Sequence) است، نگهداری می‌کند. یکی از کاربردهای معمول MBR اجرای اتوماتیک یک برنامه کاربردی در مرحله آغاز به کار سیستم است و این امر می‌تواند به‌طور اتوماتیک ویروس را فعال سازد. برخی از ویروس ها محل کد MBR را تغییر می‌دهند و کد آلوده خود را جانشین آن می‌کنند. بنابراین می‌توانند کنترل کامپیوتر را در همان ابتدای کار راه‌اندازی، پیش از اجرای برنامه های ضد ویروس به دست گیرند.

ویروس ها اغلب برنامه‌های فایل‌های فرمان (با پسوندCOM.) را آلوده می‌کنند که به کدهای اجرایی دسترسی سریع دارند. ویروس می‌تواند این روش دسترسی را ذخیره کند و آن را به کد خود تبدیل سازد. پس هر گاه برنامه آلوده اجرا شود در واقع کد ویروس اجرا می‌شود و در پایان با استفاده از آدرس ذخیره شده به ابتدای برنامه اصلی می‌رود.

تخصصی عالی و زمان کافی و منابع بسیار نیاز است . همه یا بخشی از سیستم کامپیوتر ممکن است برای مدت طولانی از کار بیفتد و برنامه‌ها و اطلاعات مهم احتمالاً از دست می‌روند. ویروس هر چه زمان بیشتری در سیستم باقی بماند فرصت بیشتری برای گسترش خواهد داشت و امکان بازسازی کاهش می‌یابد.

بدتر از آن ، کامپیوتر ممکن است به یک شبکه یا سیستم دیگری که از اطلاعات و فایل‌های برنامه به‌صورت مشترک برای چندین کاربر استفاده می‌کند متصل باشد . یک فایل آلوده در سرویس دهنده شبکه می‌تواند تمام ایستگاههای شبکه را نیز آلوده سازد. اگر آلودگی از تمام ایستگاه همزمان زدوده نشود ، مجدداً مسأله آلودگی تکرار و این سیکل دوباره آغاز می‌شود.

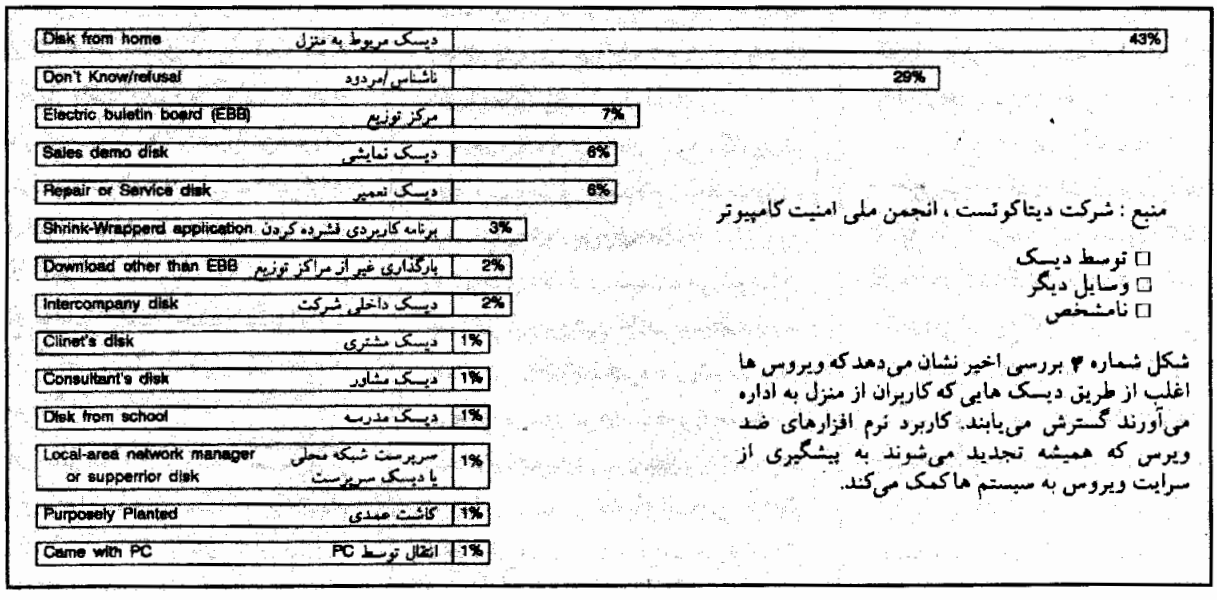
تمام برنامه‌های آلوده کننده به سیستم عاملی که برایشان نوشته شده‌اند وابستگی بسیار نزدیک دارند، در نتیجه، روش و معیارهای جلوگیری از اجرا و رشد ویروس‌ها ، خاص هر سیستم اند ، با این حال تنها چند راهنمایی کلی را می‌توان به کار برد.

کلمات رمز معمولاً در قلب اکثر سیستم های حفاظتی کامپیوتر قرار دارد و بهتر است کاربران کلمه‌های رمز خود را به دقت انتخاب کنند. حساب بسیاری از کاربران را در استفاده از کامپیوتر می‌توان از طریق ردیابی گونه‌های کلمات رمز ، مورد تعرض قرار داد مانند: نام حساب ، نام حساب توأم با خودش، نام کوچک یا خانوادگی کاربر با یک حرف بزرگ اول ، نام کوچک و یا خانوادگی کاربر با حروف کوچک و معکوس نام حساب. یک کلمه رمز خوب نباید قابل حدس باشد ، نباید در فرهنگ لغت یافت شود و باید به‌طور منظم عوض شود و به آسانی در ذهن جای گیرد .کلمات رمز تهیه شده توسط کاربران به ندرت با سه شرط اول تطابق دارد و کلمات رمز تولید شده توسط کامپیوتر فاقد شرط آخر است .

برنامه‌هایی مانند Password در سیستم های یونیکس که به کاربران امکان می‌دهند کلمه رمز تنظیم کنند باید برای عدم پذیرش انتخاب‌های عمومی اصلاح شوند و کلمات رمز پس از یک مدت زمان مشخص به‌طور اتوماتیک منقضی شوند. برخی سیستم‌ها کلمات رمز کاربران را تبدیل نمی‌کنند و حتی برخی که از ارقام یک طرفه استفاده می‌کنند تنها در برابر سوءاستفاده‌های عادی و نه حملات جدی مقاومت می‌کنند. یک نفر اخلالگر در دسترسی به فایل کلمات رمز سیستم ، اغلب می‌تواند به آسانی ، بسیاری از کلمات رمز را دریابد . آنچه که نیاز دارد تبدیل کلمات فرهنگ لغات سیستم به کد و مقایسه نتایج با کلمات تبدیل شده در فایل کلمات رمز سیستم است .

اگر چه بسیاری از سیستم‌ها در محیط مساعد و راحتی کار می‌کنند ، اما سرپرستان و کاربران ارشد سیستم باید با فن حفاظت سیستم آشنا باشند . تغییرات اعمال شده در سیستم عامل برای راحتی سرپرستان محلی، اغلب ضعف هایی را به‌وجود می‌آورد که توسط برنامه‌های مخرب یا افراد اخلالگر قابل بهره برداری‌اند . نمونه‌هایی از این گونه کارها عبارتند از : تغییر مسیر جستجو برای تسهیل کاربر و سیستم به وسیله برنامه نویسان سیستم و سرپرستان ، فراهم نمودن اجازه دسترسی به منظور نوشتن اطلاعات در سیستم ، تنظیم فایل‌های مجوز دسترسی به منظور آسان کردن انتقال فایل‌ها بین سیستم‌ها و ایجاد ارتباط راه دور .

اگر سیستم تنظیم شده باشد . روال عملیاتی ایمن‌تر مستلزم کلمه رمز است



شکل شماره ۴ بررسی اخیر نشان می‌دهد که ویروس ها اغلب از طریق دیسک هایی که کاربران از منزل به اداره می‌آورند گسترش می‌یابند. کاربرد نرم افزارهای ضد ویرس که همیشه تجدید می‌شوند به پیشگیری از سرایت ویروس به سیستم ها کمک می‌کند.

تا پیش از اعمال هر گونه تغییر در برنامه‌های سیستم و یا نصب برنامه‌های جدید ، وارد شود. انتقال فایل‌ها نیز باید از طریق کلمه رمز و نه فایل‌های مجوز انجام گیرد.

کاربران سیستم باید برای آگاهی بیشتر از روش حفاظت ، آموزش لازم را ببینند. مطالعات اخیر نشان می‌دهد که اکثر ویروس‌ها توسط دیسک‌هایی که کاربران در سیستم قرار می‌دهند و یا به دیگران اجازه این کار را می‌دهند ، منتقل می‌شوند. (شکل شماره ۴)

انجام عملیات قیاسی معمولاً مفید است ، کاربران باید از قبول نرم‌افزارهای غیرمطمئن از منابع غیر موثق پرهیز کنند. آنها نباید از افرادی نرم افزار تهیه کنند که استانداردهای حفاظتی را رعایت نمی‌کنند و باید همواره برنامه‌هایی را برای بررسی ویروس‌های مختلف شناخته شده به کار ببرند. همچنین باید در مورد نرم‌افزارهای عمومی و برنامه‌های ارسالی توسط پست الکترونیکی محتاط باشند. این عادت نیز بجاست که آخرین تاریخ اصلاح برنامه‌ها و فایل‌ها در سیستم‌ها مورد توجه قرار گیرد.

جالب است که یکی از وسایل گسترش و پخش ویروس‌ها دیسک حاوی برنامه‌های رفع اشکال کامپیوتر است . ویروس‌های متعددی مسایل و مشکلات سخت افزاری را شبیه سازی می‌کنند بنابراین یک کامپیوتر آلوده به ویروس ممکن است چنین به نظر برسد که مشکل سخت افزاری دارد. برای تشخیص مسأله ، کارشناس، دیسک عیب‌یاب را در کامپیوتر قرار می‌دهد و این دیسک نیز که به همان ویروس آلوده شده است وقتی در کامپیوتر دیگری قرار گیرد آن را نیز آلوده خواهد کرد، در نتیجه این دیسک‌ها نیز باید پس از استفاده از نظر ویروس‌ها مورد بازبینی قرار گیرند.

اگر ویروسی در محیط کامپیوتر قرار گرفته باشد و کار کپی برداری بدون بررسی و احتیاط لازم انجام گیرد ، تهیه فایل‌های پشتیبان سیستم بی‌اثر خواهد بود زیرا احتمال دارد شرایط مسئله ساز ماهها و یا حتی سالها پس از آلودگی اولیه ایجاد شود . بازیابی اطلاعات پشتیبان می‌تواند به سادگی آلودگی را تجدید نماید.

برنامه‌های ضدآلودگی

در بسیاری از موارد ، برنامه‌های

Microprocessor	Alpha 21064	MIPS R4400SC	PA7100	Pentium	PowerPC 601	Super Space	68040	80486
company	Digital Equipment Corp.	Mips Technol – Ogies Inc.	Hewlett Packard Co	intel Corp	IBM Corp. and Motorola Inc	Sun Micro - systems Corp.and Texas Instru-ments Inc	Motorola Inc.	intel Corp
Introduction data	2/92	11/92	2/92	3/93	4/93	5/92	1989	6/91
Architecture and organization								
Type	RISC	RISC	RISC	CISC	RISC	RISC	CISC	CISC
Width,bits (a)	64	64	32	32	32	32	32	32
On-chip cache,kB (instruction/data)	8/8	16/16	None	8/8	32 unified	20/16	4/4	8 unified
Off-chip cache,MB (instruction/data)	16	4	1/2	External controller	External controller	External controller	External controller	External controller
No.of registers (general-purpose /FP)	32/32	32/32	32/32	8/8	32/32	136/32	16/8	8/8
Instruction issue rate per cycle	2	1	2	2	3	3	1	1
No.of independent units	4	N.A.	3	3	3	5	N.A	N.A
No of pipeline stages (integer /FP)	7/10	7/10	5/6	5/8	4/6	4/5	3/6	5/N.S.
Endian (b)	little	Big/little	Big	Little	Big.little	Big	Big	Little
Typical latency (integer /FP)	1/8	1/4	1/2	1/3	1/3	1/3	1/3	N.S.
Multiprocessing support?	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Technology and perrormance								
Technology	0.68 μm CMOS	0.6 μm CMOS	0.8 μm CMOS	0.8 μm BiCMOS	0.65 μm CMOS	0.7 μm BiCMOS	0.65 μm CMOS	0.8 μm CMOS
Die size,mm	15.3 by 12.7	12 by 15.5	14.2 by14.2	17.2 by17.2	11 by 11	18 by 16	10.8 by11.7	N.S.
Transistors,millions	1.68	2.3	0.85	3.1	2.8	3.1	1.2	1.2
Metalization layers	3	2	3	3	4	3	2	3
Operating voltage,V	3.3	5/3.3	5	5	3.6	5.3	5	5
Clock, MHz	200	150	100	66	80	60	25	50
SPECint 92 (c)	130	88	81	67.4	85	80	21	27.9
SPECfp 92 (c)	184	97	150	63.6	105	100	15	13.1
Power,packaging,and price								
Peak power,W	30	15	23	16	9.1	142.2	6	5
Cooling	Heat sink	Heat sink	Heat sink	Fan plus heat sink	Ambient plus heat sink	Forced air plus heat sink	Amvient . plus heat sink	Fan or heat sink

انواع ریزپردازشگرهایی که به تازگی به بازار آمده‌اند

برای گسترش ویروس ، کد آن باید به طور مستقیم با اجرای برنامه آلوده اجرا شود و یا به عنوان بخشی از ردیف راه‌اندازی سیستم و یا به صورت فعالیت پس زمینه فعال شود.

بسیاری از ویروس‌های شناخته شده اگر اجرا شوند ؛ حتی اگر اجرای برنامه میزبان آنها به پایان رسیده باشد در حافظه باقی می‌مانند. یک ویروس مقیم در حافظه ، خود را در بلوکی از حافظه کپی کرده سیستم وقفه استاندارد را که توسط DOS و BIOS به کار می‌رود تغییر می‌دهد. سپس هنگامی که برنامه‌های کاربردی سیستم وقفه را برای پاسخگویی به درخواست‌های سیستم عامل به‌کار می‌برند ناآگاهانه ویروس را به فعالیت درمی‌آورند. بدین ترتیب ، اگر یک برنامه آلوده به ویروس اجرا شود همه برنامه ها را نیز آلوده خواهد کرد. این گسترش و سرایت ویروس در تمام مدت یک دور کار ادامه می‌یابد.

بمب های منطقی (Logical Bombs)

بمب های منطقی دقیقاً برنامه‌هایی هستند که معمولاً به خواب فرو می‌روند تا بر اثر تأمین شرطی خاص "منفجر" می‌شوند و فایل‌های کامپیوتر میزبان را تخریب می‌کنند. بمب های منطقی می‌توانند در اسب تروا (Trojan Horse) مقیم شوند و یا توسط ویروس‌ها انتقال یابند. این بمب‌ها وسایل مطلوبی برای انتقامجویی کارمندان ناراضی و پیشین هستند به طوری که می‌توانند این برنامه‌ها را هنگامی که در شرکت حضور ندارند به فعالیت در آورند. شرط فعال شدن بمب (انفجار) می‌تواند حذف کردن نام کارمند اخراجی از رکوردهای سیستم حقوق باشد. معمولاً حداکثر خسارت در زمانی کوتاه وارد می‌شود.

این گونه عملیات تأخیری، برای اخاذی مالی نیز به کار می‌رود و معمولاً این پیغام ظاهر می‌شود :"پول را پرداخت کنید تا محل اختفای بمب در اختیارتان قرار گیرد". افزون بر آن ، تولیدکنندگان و مشاوران که سیستم کامپیوتری را تنظیم می‌کنند ، برای دریافت صورت حساب‌های مالی خود از این ابزار استفاده می‌کنند تا در صورت دریافت نکردن مطالبات خود، بمب منفجر شده سیستم را فلج کند. این روش وحشت انگیز وقتی که یکی از کتابخانه‌های مریلند از پرداخت وجوه مربوط به یک سیستم ناکارآمد امتناع کرد به کار افتاد اما بمب قبل از این که خسارتی به بار آورد کشف شد.

بمب‌های منطقی را برای کاربران خاص نیز به کار می‌برند مثلاً ویروس اسکورز (Scores Virus) /که ویروس خاص سیستم مکینتاش است و توسط کارمندان اخراجی شرکت سیستم داده‌های الکتریکی (EDS) در دالاس به منظور انتقامجویی تهیه شد./ تمام برنامه‌های کاربردی را آلوده می‌ساخت و حجم آنها را افزایش می‌داد، هر سه و نیم دقیقه میزبان جدیدی برای آلوده سازی پیدا می‌کرد، دنبال تمام فایل‌های خاص حاوی اطلاعات کارمندان شرکت EDS می‌گشت و آنها را نابود می‌کرد و بالاخره سرعت سیستم را کاهش می‌داد و مشکلاتی در امر چاپ و شکل نشان‌های خاص پدید می‌آورد.

کرم ها(Worms)

کرم ها برنامه هایی هستند که در یک شبکه کامپیوترها از ایستگاه یا کامپیوتری به ایستگاه یا کامپیوتر دیگر انتقال می‌یابند و یا سفر می‌کنند. آنها نخستین بار در مرکز پژوهشی پالوآتوی شرکت زیراکس (PARC) به عنوان ابزاری برای انجام کاری مفید، روی شبکه توزیع اطلاعاتی مانند اطلاعات پیکربندی سیستم در محیط غیرمتمرکز، به‌وجود آمدند.

برنامه‌های کرم با استفاده از مزایایی که منابع مطابق با آنها، در یک شبکه کامپیوتری به‌طور مشترک به‌کار می‌روند حرکت می‌کنند و در برخی موارد نواقصی در نرم افزار استاندارد نصب شده در سیستم شبکه پدید می‌آورند. کرمی که در یک کامپیوتر متصل به شبکه اجرا می‌شود دنبال میزبانان دیگری درون شبکه می‌گردد و هرگاه یک مورد پیدا کند پیوند ارتباطی با سیستم راه دور ایجاد می‌کند و "برداری" (Vector) شامل کد راه‌اندازی ارسال می‌نماید. این بردار آنگاه پیوند ارتباطی بازگشتی با سیستم آلوده ایجاد می‌کند و میزبان جدید نسخه‌هایی از فایل‌هایی را که بدنه اصلی کرم را تشکیل می‌دهند بارگذاری می‌کند.

با براندازی و اخلال در اجرای سیستم‌های شبکه ، انحصاری کردن منابع و ایجاد پیوندهای ارتباطی در شبکه ، کرم ها حتی اگر ظاهراً مخرب هم نباشند قادر به فلج کردن شبکه هستند. غالباً ، تمام شبکه کامپیوترها پیش از بازسازی کلاً از کار می‌افتد.

یکی از راه هایی که کرم انتشار می‌یابد توسط کرم اینترنت (Internet) به‌کار گرفته می‌شود که سیستم‌های یونیکس شبکه اینترنت ایالات متحده آمریکا را در تاریخ دوم نوامبر ۱۹۸۸ آلوده‌کرد . اگر کرم به سیستم سرایت کند شروع به گردآوری اطلاعاتی در باره میزبانان دیگر مرتبط با سیستم می‌کند سپس برای آلوده سازی این میزبانان، سه عمل انجام می‌دهد: نخست سعی می‌کند با استفاده از فرمان rsh در یونیکس با سیستم مقصد مرتبط شود. در صورت موفقیت یک پروتکل کنترل انتقالی (TCP) به کامپیوتر آلوده بازمی‌گرداند به طوری که برنامه بردار می‌تواند به مقصد ارسال و ترجمه و اجرا شود. آنگاه بردار همراه با کرم موجود در سرویس دهنده برای کپی

ویژگیهای مربوط به پردازشگرهای جدید

Characteristic	Capability
Instructions Length Number of formats	32 bits <= 2
Addressing modes	<=3
Indirect addressing?	None
Register files	>=32
Operations (except memory access)	Register-to-register
Memory operations across page boundaries?	None
Memory access	Load/Store

کردن بدنه کرم واقعی در مقصد که ترجمه ، لینک و اجرا شده است به فعالیت می‌پردازد. کرم پس از حصول اطمینان از موفقیت‌آمیز بودن آلوده سازی، ارتباط خود را قطع می‌کند.

اگر روش اول توأم با موفقیت نباشد، کرم سعی می‌کند توسط اشباع بافر ورودی با رشته مخصوص ۵۳۶ بایتی در برنامه انگشتی (Fingered) نقصی ایجاد کند. یک فرآیند انگشتی معمولاً همانند یک روح خبیث عمل می‌کند تا اطلاعاتی راجع به کاربران دیگر مانند نام کامل و یا شاید شماره تلفن دسترسی ، گردآوری کند. این عمل از تابع gets مجموعه C برای خواندن داده‌ها استفاده می‌کند ؛ gets تمام رشته ورودی را بدون بررسی سرریز شدن بافر می‌خواند. سرریز شدن باعث می‌شود ناحیه‌ای از پشته (Stack) سیستم مورد بازنویسی واقع شود و کرم بتواند دستورالعمل‌هایی در پشته قرار دهد تا زمان اجرا از طریق TCP ارتباط راه دور ایجاد شود . سپس مطابق با توضیحات بالا آلودگی انتشار می‌یابد.

اگر هر دو روش یاد شده موفقیتی به دست ندهند ، کرم سعی می‌کند به درگاه SMTP (Simple Mail Transfer Protocol) مربوط به کامپیوتر دوردست مرتبط شود. برنامه کمکی پست الکترونیکی یونیکس ، یعنی Sendmail برای دریافت پست به این درگاه (Port) مراجعه می‌کند. یک گزینه برای برنامه Sendmail فرمان DEBUG است که به آزمایش کنندگان برنامه امکان می‌دهد دریافت پست در یک مرکز را بدون فعال کردن روتین‌های آدرس پست کننده بازبینی کنند. بسیاری از فروشندگان و مدیران ، گزینه اشکال‌زدایی ترجمه شده در کد Sendmail می‌گذارند تا پیکربندی پست کننده در شرایط محلی تسهیل شود. کرم فرمان DEBUG را به Sendmail ارسال می‌کند و سپس یک رشته فرمان ها را برای پست کردن بردار به سیستم مقصد فعال می‌کند و آن را به اجرا درمی‌آورد. بدنه کرم سپس به همان طریق انتقال می‌یابد.

اگر کرم انتقال یابد ، اولین کار کرم استتار وجود خود است و علاقه‌ای به نسخه دودویی خود ندارد و با از میان بردن فرآیند اصلی خود فایل‌هایش را وارد حافظه می‌کند ، آنها را می‌پوشاند ، فایل های ایجاد شده در زمان ورود به سیستم را حذف می‌کند و سپس شروع به دخالت منظم در حساب‌های کاربر با استفاده از فایل کلمات رمز یونیکس و تمام کاربران برای انتخاب کلمات معمول به‌عنوان کلمه رمز می‌کند. اگر کلمه رمز کاربری را پیدا کند می‌تواند خود را زیر نقاب کاربر قرار دهد و به کامپیوترهای دوردستی که کاربر در آنها حساب دارد دسترسی یابد.

کرم گاهی مشابه خود را ایجاد می‌کند و اصل را از بین می‌برد به طوری که مشخصات آن همواره تغییر می‌کند. این کار از تخصیص مقدار زیادی از وقت واحد پردازش مرکزی (CPU) توسط یک فرآیند جلوگیری می‌کند و اطمینان حاصل می‌شود که اولویت زمانبندی آن برای استفاده از زمان زیاد CPU تنزل نخواهد کرد. هر ۱۲ ساعت ، رکورد مربوط به میزبانان آلوده شده را پاک می‌کند ، بنابراین یک کرم تک می‌تواند پس از ۱۲ ساعت همان میزبان را مجدداً آلوده کند.

باکتری

کاربرد این کلمه برای یک برنامه مخرب نسبتاً جدید است و برخی پژوهشگران ویروس ترجیح می‌دهند آنها را در رده ویروس‌ها قرار دهند. دیگران نیز سعی دارند رده‌ای غیر از ویروس به آنها اختصاص دهند زیرا اینها به برنامه میزبان نیاز ندارند.

یک برنامه باکتری به سادگی سعی می‌کند خود را تکثیر کند و تا جایی که امکان دارد به زمان بیشتری از CPU نیاز دارد تا سیستم میزبان خود را کُند نماید (با اجرای نسخه‌های مختلف خودش) و نیز ممکن است دیسک را پر از نسخه‌های خود کند. باکتری کریسمس آی بی ام یک نمونه از باکتری‌ها است که در دسامبر ۱۹۸۷ به بیت نت (Bitnet) شبکه دانشگاهها حمله کرد /دانشگاههای نیویورک و ییل/. این باکتری تصویر یک درخت کریسمس را روی صفحه نمایش نشان می‌داد و در عین حال از سیستم پست الکترونیکی شبکه برای توزیع نسخه‌های خود بین کاربران مختلف استفاده می‌کرد. رشد آن به‌صورت هندسی بود و سریعاً سیستم را کُند می‌کرد و قبل از این که همه نسخه‌های برنامه از بین بروند آن را کلاً متوقف می‌کرد.

پیشگیری و معالجه

بازسازی سیستم آلوده به ویروس کار آسانی نیست . برای این کار به کپی

کمکی پاکسازی ویروس قادر به پاک کردن ویروس از سیستم هستند. این برنامه‌ها نخست سعی می‌کنند نوع ویروس را توسط مقایسه نشانگذار آن سپس با به‌کار گیری شناخت و دانش کافی نسبت به روش آلودگی و ساختار برنامه شناسایی کنند.

برای نمونه ، در مورد ویروس‌هایی که دستورالعمل های پرش (Jump) را در ابتدای برنامه میزبان تغییر می‌دهند، بازسازی می‌تواند به سادگی بازیابی پرسش اصلی به ابتدای کد میزبان باشد. بهترین برنامه‌های ضدآلودگی می‌توانند چند ضد ویروس مختلف را شناسایی کنند و اغلب به محض کشف ویروس‌های جدید به روز می‌آیند.

با این حال غالباً ساده‌ترین راه برای "معالجه" یک کامپیوتر آلوده به ویروس، توقف کار و سپس جستجو و بررسی حافظه و همه دیسک‌های آن و بازسازی فایل‌ها است . برنامه‌ها باید از نسخه اصلی بارگذاری شوند و دیسک‌های نو باید دقیقاً مورد بازبینی قرارگیرند.

برنامه‌های متعدد مصون سازی به عنوان "واکسن" بر ضد ویروس‌ها و اسبان تروا مورد استفاده قرار می‌گیرند. واکسیناسیون با اصلاح هر برنامه در کامپیوتر و درج مکانیسم آزمایش خودکار عمل می‌کند. این مکانیسم از روش‌های الگوریتمی و سر جمع زدن مشخص می‌کند که آیا نظم دستورالعمل‌ها در برنامه تغییر کرده است یا خیر ؟ این آزمایش خودکار هر بار که برنامه اجرا شود این مطلب را بررسی می‌کند که آیا از آخرین بار اجرا تغییری در آن پدید آمده است یا خیر؟

مؤثرترین آزمایش های خودکار از روش کد کردن عمومی و نشان‌های دیجیتال (رقمی) برای محاسبه سرجمع براساس فایل‌های مقصد (Object) که به وسیله صاحب اصلی به کمک کلید مخفی خود نشانگذاری شده‌اند استفاده می‌کنند. سیستم عامل می‌تواند سلامت فایل‌ها را توسط کلید عمومی صاحب بررسی کند. برنامه‌های آلوده شده به وسیله ویروس نمی‌توانند این آزمایش را با موفقیت پشت سر بگذارند.

روش‌های دیگر برای نگهداری سیستم‌ها روی خنثی کردن عملیات مخرب برنامه‌های مضر متمرکز شده‌اند. برای نمونه برای کنترل حذف فایل یا تغییر برنامه ، سیستم عامل می‌تواند از کاربر، مجوز لازم را برای کار با برنامه یا تغییر برنامه یا فایل درخواست کند. با این حال ، این روش خسته کننده است و در بسیاری از موارد مؤثر نیست زیرا کاربر یک برنامه بزرگ /همانند یک واژه‌پرداز/ ممکن است نداند کدام فایل‌ها مجاز به تغییر هستند.

سخت افزارهای حفاظت از حافظه که یک برنامه را در ناحیه خاصی از حافظه محدود می‌کنند ، ممکن است احتمال حمله تخریبی راکاهش دهند. با این حال ، برخی ویروس‌ها می‌توانند به‌طور مشروع در برنامه‌های قابل دسترسی از جمله بخش‌هایی از سیستم عامل نفوذ کنند.

یک روش مؤثر برای کشف آلودگی ویروس استفاده از "برنامه عکس‌بردار" (Snapshot Program) است که همه اطلاعات مهم سیستم را در زمان نصب اولیه ثبت می‌کند. سپس یک روتین بازبینی به‌طور دوره‌ای برای مقایسه وضعیت فعلی سیستم با تصویر اصلی اجرا می‌شود . اگر نشانه‌های آلودگی کشف شوند ، ناحیه تحت تأثیر کامپیوتر شناسایی و به کاربر تند کار داده می‌شود.

روش " طرح آدرس شاخه‌ای " (Branch Address Maps) نیز مفید است و برای بررسی برنامه‌های قابل اجرا از نظر آلودگی ویروسی به‌کار می‌رود. این روش حدود فضای آدرس مربوط به همه در خواست های سرویس برنامه‌ها نظیر فراخوانی سیستم عامل و وقفه‌های سیستم را پیگیری می‌کند، و قادر است چند صد برنامه را در چند ثانیه مورد بازبینی قرار دهد.

در باره مؤلفان

جان بولز (John B. Bowles) استادیار دپارتمان مهندسی برق و کامپیوتر دانشگاه کارولینای جنوبی (USC) در کلمبیا است و مباحث مربوط به طراحی سیستم‌های مطمئن را تدریس می‌کند و مورد پژوهش قرار می‌دهد. پیش از پیوستن به USC ، سرپرست پروژه گروه تحلیل سیستم‌ها، توسعه سیستم‌های پیشرفته در شرکت NCR و یکی از اعضای کارشناسی آزمایشگاه بل (Bell) بود.

کولن پلائز (Colon E. Pelaez) دانشجوی دوره دکترای مهندسی برق و کامپیوتر در دانشگاه کارولینای جنوبی و عضو دانشکده اسکولاسوپریور پلی‌تکنیکال لیتورال در گویاکوئیل اکوادور است . او دستیار فنی سنترود سرویسیوس کومپیوتاسیونالس و مسئول نگهداری شبکه PC ها است .